Surveillance in the digital age: Exploring positive outcomes of surveillance in the form of group-based recognition

Submitted by Josephine Ann Cooper to the University of Exeter

as a thesis for the degree of

Doctor of Philosophy in Psychology

In February 2020

I certify that all material in this thesis which is not my own work has been identified and that no material has previously been submitted and approved for the award of a degree by this or any other university.

Signature: ……

ACKNOWLEDGMENTS

There are several special people who made it possible for me to complete this thesis and the research within it. I would first like to thank my supervisors, Andrew Livingstone and Mark Levine. Thank you for giving me the opportunity to embark on this research and for your encouragement throughout. I feel privileged to have learned and gained inspiration from your own enthusiasm, knowledge, and expertise. Aside from academic guidance, I would also like to express my sincere gratitude for the kindness you have both given me throughout this project. Outside of my research team, I would like to thank the SEORG group at Exeter; your advice and insight helped shaped this thesis. I am particularly grateful to Anna Rabinovich and Teri Kirby for their invaluable guidance at my upgrade.

My fellow PhD students at Exeter have also provided me with support and friendship whilst I worked on campus. I would like to thank everyone, especially for the much-needed trips to the campus shop to get some air and normalcy. A special thanks goes to Asha Ladwa, who was a sister to me whilst we shared an office together. I'll always miss our gym sessions and cooking extravaganzas. I am also hugely grateful to Denise Wilkins, my mentor and friend; you are and have been relentlessly supportive.

Finally, I would like to thank those that have been by my side throughout the PhD and beyond. My parents, Sandra and Stephen Cooper, have been my cheerleaders throughout life. I am beyond lucky to have won the parental lottery and feel proud to call you mamgu (sorry!) and dad. I would also like to thank my brother, Bevis. Our marathon phone calls putting the world to rights have

reminded me that there is life outside my PhD. My good friend Henry Maher also deserves a special thank you for never failing to make me laugh (and for being the best research assistant one could ask for). A big thank you also goes to my best friend Emma Banbrook. You are continually a beacon of support and confidence. Lastly, but certainly not least, I would like to thank my husband Will, who has been unfathomably patient, loving, and encouraging throughout this process.

ABSTRACT

Narratives surrounding algorithmic surveillance typically emphasise negativity and concerns about privacy. In contrast, we argue that current research underestimates potentially *positive* consequences of algorithmic surveillance in the form of group-based recognition. Specifically, we test whether (accurate) algorithmic surveillance (i.e., the extent to which those surveilled believe surveillance mirrors their own self-concept) provides a vehicle for group-based recognition in two contexts: (1) those under outgroup surveillance and (2) surveillance from the perspective of stigmatised and misrecognised groups. In turn, we test whether this can lead to more positive (and less negative) feelings towards surveillance. Alongside this, we also test whether a countervailing negative pathway exists, whereby more accurate surveillance is associated with more privacy concern, and in turn, more negative (and less positive) feelings towards surveillance. The final study also tests whether positive perceptions of accurate surveillance arising through group-based recognition are limited only to misrecognised groups, or whether this is true for people more generally. Across seven studies, we test the core hypothesis that group-based recognition from accurate surveillance provides a basis for positive reactions to algorithmic surveillance that countervails the negative pathway through privacy concern. Overall, we found support for the positive pathway, whereby more accurate surveillance was associated with more positive feelings towards surveillance through group-based recognition. The positive pathway was present for both typically recognised and misrecognised groups. We also found partial support for the negative pathway; whereby privacy concern was associated with less positive feelings towards surveillance. However, we did not find that surveillance accuracy was

associated with privacy concern; one implication of this is that the presence of surveillance per se overwhelms any additional effect of surveillance accuracy. Additionally, surveiller social identity (ingroup vs. outgroup) influenced both the positive and negative pathways: surveillance from an outgroup was considered less trustworthy than ingroup surveillance, which in turn predicted less positive outcomes in the form of more privacy concern and less group-based recognition. This thesis challenges the current techno-pessimistic view that algorithms are inherently negative and contributes to research that endeavours to gain a greater understanding of society's relationship with algorithms and artificial intelligence.

GENERAL INTRODUCTION AND SUMMARY

Processes that contribute towards the public's feelings towards algorithmic surveillance are poorly understood. Modern forms of surveillance use algorithms, which are integral to the online surveillance architecture. Algorithmic surveillance enables organisations (both corporate and state) to gather and analyse our online behaviour through code (or a set of rules), which use data to produce a specified output (Sandvig, Hamilton, Karahalios, & Langbort, 2015). Within a surveillance context, algorithms scan individuals' data to identify patterns or correlations (Tene & Polonetsky, 2014), which are then used to categorise people into social groups. From these groups, organisations infer our characteristics and make predictions about our future behaviour (Lyon, 2003). Ultimately, algorithmic surveillance allows companies to recognise who we are, and to tailor their response accordingly.

Websites often claim that algorithmic surveillance will 'improve the user experience' (Unidrain, 2018, para. 5), as material can be 'tailored to your own specifications' (The Independent, n.d., How do we use cookies section, para. 1) to ensure it is 'relevant and engaging' (Bright Horizons, n.d., Marketing section, para. 1). In other words, users are assumed to feel more positively towards surveillance, as it can recognise who they are and what they want. These narratives surrounding commercial surveillance highlight the potential for both positive and negative outcomes. On one hand, users are offered the opportunity of greater recognition, yet on the other hand the harvesting of users' data may threaten privacy. This thesis examines whether these two countervailing processes contribute to users' feelings towards surveillance. Additionally, we predict that the accuracy of surveillance (i.e. the extent to which targeted material reflects the user's identity) will affect these outcomes: individuals may

simultaneously experience more privacy concern and recognition when surveillance is of greater accuracy. In this instance, accurate algorithmic surveillance functions as a double-edged sword, providing both positive and negative psychological outcomes.

Privacy concern

Surveillance has historically prompted discussions surrounding privacy. Digital privacy advocates argue that online mass surveillance threatens both individual liberty (Gillmor, 2014) and national security (Schneier, 2016). Some have taken this further: in 2015, the United Nations privacy chief accused surveillance practices of being worse than the dystopia illustrated in Orwell's *1984* (Culpan, 2015). Indeed, the growing concern for our online privacy has given rise to groups and movements dedicated to restoring online freedom. For example, the protest 'The Day We Fight Back' aimed to protect user privacy by exerting pressure on US law makers to restrict the state's ability to engage in mass surveillance (Gillmor, 2014). Additionally, The American Civil Liberties Union (ACLU) has campaigned to end the United States of America (USA) Patriot Act, which gives the government greater powers to collect data from those who are not necessarily under suspicion (ACLU, n.d.). Algorithmic surveillance can thus in some circumstances create concern for privacy online, and this in turn can create animosity towards those surveillance systems.

Recognition

However, an alternative narrative (typically put forward by those conducting commercial surveillance) argues that algorithmic surveillance can foster positive feelings towards surveilling platforms, as it can enhance user recognition. In particular, this thesis focuses on group-based recognition: the

extent to which others (specifically those from other groups) perceive the ingroup in a way that reflects the ingroup's own self-concept (Tajfel, 1981).[1]

For example, the cookie disclaimer is a familiar form of algorithmic surveillance and an inevitable part of the online landscape for many internet users. The cookie pop-up notifies users that the website employs surveillance, and that continued use of the site implicitly provides consent to this. Prior to the cookie warning, data collection practices were unbeknownst to many internet users (Friedland & Sommer, 2010). Many became alarmed once they learned of these surveillance practices (Vega, 2010), which prompted the European Union (EU) to implement 'The Cookie Law' in May, 2011. Once passed, this ordered companies conducting surveillance to gain consent from site visitors. The law was designed to increase transparency by informing users how their data were being collected and used (OneTrust, n.d).

Whilst this was the original purpose of the cookie pop-up, many companies have since used the disclaimer as an opportunity to advocate what they believe is a key benefit of surveillance: recognition. This has contributed to the alternative discourse that suggests surveillance is beneficial for users because user recognition is enhanced. For example, Facebook argues that relevant (targeted) material on their platform enhances user experience; the relevance of an advert is calculated by assessing how similar the content of the advert is to the user's (inferred) attitudes (Facebook, 2015). Users are then only shown content that aligns with their predicted preferences. In essence, Facebook expects individuals to feel more positively about the platform when their beliefs are recognised in some capacity. Similarly, in 2012 Google made controversial changes to its privacy policy, resulting in the consolidation of

[1] The definition and concept of group-based recognition is explored in greater depth in Chapter 1.

users' data across its product lines (e.g. Google search engine, Gmail, and Youtube). Google defended the changes, arguing that this enabled them to better recognise users' interests and in turn tailor content across services (Melvin, 2012). Whilst Google and Facebook likely have profit-driven motives for increasing user recognition, the assumption that surveillance can increase group-based recognition, and in turn increase favourability towards surveillance, has not yet been tested.

Surveillance accuracy

Both narratives surrounding privacy and recognition typically assume that to some extent surveillance gets us right. In other words, increased privacy concern and/or recognition are inevitable outcomes of surveillance. This may not always be the case, as the accuracy of surveillance can vary considerably. For example, Itrona and Wood (2004) claim that surveillance systems can be infused with human biases, whereby social groups are associated with stereotypical behaviours and beliefs. They argue these biases are also likely to go unnoticed, as algorithms are assumed to be neutral in their decision making. Additionally, they suggest that human operators are less likely to intervene if they suspect an error with an algorithm, as the system is assumed to hold more authority due to its perceived sophistication.

Surveillance accuracy may also vary because of the quantity of data collected. For example, Murphy (2017) suggested that data become unmanageable when collected in vast amounts, even when analysis is automated using algorithms. As a result, online profiles can become decontextualized versions of users' 'real' self and similarities to others can become exaggerated (de Zwart, Humphreys, & Dissel, 2014). Indeed, some within the National Security Agency (NSA) have acknowledged that the deluge

of information collected can increase the likelihood of errors in data interpretation (Maass, 2015). Consequently, the accuracy of surveillance may vary depending on how much data is collected and the subsequent design and application of algorithms used to analyse it.

In light of this, we predict that variation in perceived surveillance accuracy may affect the degree to which internet users experience privacy concern and group-based recognition. Greater surveillance accuracy may be associated with an increase in privacy concern, yet simultaneously offer greater recognition. In turn, these outcomes may be associated with users' feelings towards surveillance; more privacy concern and group-based recognition should predict more negative and more positive feelings towards surveillance respectively. However, the effect of surveillance accuracy on feelings towards surveillance through privacy concern and group-based recognition have not yet been investigated.

TABLE OF CONTENTS

ACKNOWLEDGMENTS i

ABSTRACT iii

GENERAL INTRODUCTION AND SUMMARY v

Privacy concern vi

Recognition vi

Surveillance accuracy viii

LIST OF TABLES xvi

LIST OF FIGURES xviii

CHAPTER 1 1

LITERATURE REVIEW 1

Variation in feelings towards surveillance 1

The importance of understanding the processes that contribute to feelings towards surveillance 3

Predictors of feelings towards surveillance 4

Negative psychological drivers 4

Positive psychological drivers of feelings towards surveillance 15

The role of surveillance accuracy 26

CHAPTER 2 33

STUDY 1 33

Method 35

Results 40

Discussion 48
CHAPTER 3 56
Intergroup surveillance and group-based recognition 56
Effects of surveiller identity and surveillance accuracy on privacy concerns 60
The role of trust: A potential mediator between surveiller identity and psychological outcomes 62
Overview of studies 63
STUDY 2A 64
Method 65
Results 70
Discussion 78
STUDY 2B 83
Method 86
Results 90
Discussion 101
STUDY 2C 108
Method 109
Results 114
Discussion 122
GENERAL DISCUSSION 126
The positive pathway: More accurate surveillance is associated with more positive feelings towards surveillance through group-based recognition . 127

The negative pathway: More accurate surveillance is associated with more negative feelings towards surveillance through privacy concern 132

Limitations and future research..... 136

Summary 137

CHAPTER 4 140

STUDY 3A 145

Method 145

Results 149

Discussion..... 154

STUDY 3B 159

Method 160

Results 164

Discussion..... 168

GENERAL DISCUSSION..... 171

Positive pathway (1): Surveillance of greater accuracy is associated with more perceived group-based recognition 172

Positive pathway (2): Greater perceptions of group-based recognition predict more positive and less negative feelings towards surveillance 174

Negative pathway (1): Surveillance of greater accuracy is not associated with more privacy concern 177

Negative pathway (2): Greater privacy concern is associated with less positive and more negative feelings towards surveillance 179

Future research 180

CHAPTER 5 182
STUDY 4 182
Method 184
Results 189
Discussion 196
The positive pathway: (Mis)recognition does not moderate the association between surveillance accuracy and group-based recognition 197
The negative pathway: Surveillance of greater accuracy was not associated with increased privacy concern 200
Limitations and future research 202
Summary 203
CHAPTER 6 204
GENERAL DISCUSSION 204
Summary of findings 204
Positive pathway: Positive feelings towards surveillance through group-based recognition 206
Negative pathway: Negative feelings towards surveillance through privacy concern 208
Are group-based recognition benefits through accurate surveillance contingent on misrecognition? 209
Contributions of the present thesis 211
The role of accuracy 212

Positive psychological outcomes in the form of group-based recognition 213
Conceptualising group-based recognition 217
Negative psychological outcomes in the form of privacy concern..... 218
Strengths, limitations and directions for future research 220
Practical implications 224
Conclusion 229
REFERENCES 230
APPENDICES 268
Appendix A: Study 1 manipulation article 268
Appendix B: Study 1 full list of measures 272
Appendix C: Study 2a manipulation university news bulletin 281
Appendix D: Study 2a full list of measures 287
Appendix E: Study 2b manipulation university news bulletin..... 291
Appendix F: Study 2b full list of measures 297
Appendix G: Confirmatory factor analysis for the group-based recognition scale..... 303
Appendix H: Study 2c manipulation article 305
Appendix I: Study 2c full list of measures..... 317
Appendix J: Confirmatory factor analysis for the group-based recognition measure 322
Appendix K: Study 3a full list of measures 324
Appendix L: Stimulus text for Study 3a 330

Appendix M: Confirmatory factor analysis for the group-based recognition measure 332

Appendix N: Study 3b manipulation materials 334

Appendix O: Study 3b full list of measures 344

Appendix P: Confirmatory factor analyses of the group-based recognition measure 349

Appendix Q: Study 4 manipulation materials 353

Appendix R: Study 4 full list of measures 369

Appendix S: Confirmatory factor analysis for the group-based recognition measure 375

LIST OF TABLES

Table 1. Correlations between measures 41

Table 2. Multiple Regression Analysis Investigating the Relationship Between Psychological Outcomes and Feelings Towards Surveillance..... 47

Table 3. Correlations between measures 73

Table 4. Multiple regression analysis investigating the relationship between psychological outcomes and behaviour change intentions online 78

Table 5. Summary of Pearson correlations between variables in the predicted model 92

Table 6. Multiple regression analysis investigating the relationship between psychological outcomes and positive feelings towards surveillance..... 100

Table 7. Multiple regression analysis investigating the relationship between psychological outcomes and negative feelings towards surveillance 101

Table 8. Correlations between measures 115

Table 9. Multiple regression analysis investigating the relationship between psychological outcomes and positive feelings towards surveillance..... 121

Table 10. Multiple regression analysis investigating the relationship between psychological outcomes and negative feelings towards surveillance 122

Table 11. Summary of Pearson correlations between variables in the predicted model. 149

Table 12. Summary of indirect effects for positive feelings through each mediator variable in the predicted model. 153

Table 13. Summary of indirect effects for negative feelings through each mediator variable in the predicted model. 153

Table 14. Summary of zero-order correlations between variables in the analyses. 165

Table 15. Summary of Pearson correlations between dependent variables in the predicted model. 190

Table 16. Multiple regression analysis investigating the relationship between psychological outcomes and positive feelings towards surveillance..... 195

Table 17. Multiple regression analysis investigating the relationship between psychological outcomes and negative feelings towards surveillance 196

LIST OF FIGURES

Figure 1. Theoretical model demonstrating the positive and negative pathway which produce countervailing effects on feelings towards surveillance. 32

Figure 2. Predicted model with visibility as an additional mediator. 35

Figure 3. Feelings towards algorithmic surveillance as a function of surveillance accuracy. Low internet use is a score 1SD below the mean for internet use and high internet use is a score 1SD above the mean. 43

Figure 4. Privacy concern as a function of surveillance accuracy. Low internet use is a score 1SD below the mean for internet use and high internet use is a score 1SD above the mean. 45

Figure 5. The conditional effect of surveillance accuracy on behaviour change intentions at the level of surveiller identity (ingroup surveillance versus outgroup surveillance). 72

Figure 6. The conditional effect of surveillance accuracy perceptions on group-based recognition at the level of surveiller identity (ingroup surveillance versus outgroup surveillance). Low and high accuracy are valued at 1SD below and above the mean respectively. Medium is valued at the mean. 74

Figure 7. Path diagram illustrating the effect of surveiller identity on privacy concern through trust. 76

Figure 8. Path diagram illustrating the effect of surveiller identity on group-based recognition through inferred trust. 77

Figure 9. PROCESS path diagram for predicted model. Unstandardised regression coefficients and significance values are presented adjacent to each line that represents the relationship between variables. 96

Figure 10. The conditional effect of surveillance accuracy perceptions on perceived distinctiveness at the level of the ingroup and outgroup. Low and high

accuracy are valued at 1SD below and above the mean respectively. Medium is valued at the mean. 98
Figure 11. PROCESS path diagram for predicted model. Unstandardised regression coefficients and significance values are presented adjacent to each line that represents the relationship between variables. 120
Figure 12. Path model illustrating the predicted model. Rectangles represent observed scale variables. Standardised coefficients for each relationship are depicted above path arrows along with significance values. Group-based recognition dimensions were covaried, as were positive and negative feelings towards surveillance. *Note:* * $p < .05$, ** $p < .01$, *** $p < .001$. 150
Figure 13. PROCESS path diagram for predicted model. Unstandardised regression coefficients and significance values are presented adjacent to each line that represents the relationship between variables. 167
Figure 14. The conditional effect of surveillance accuracy on felt understanding at the two levels of recognition. 193

CHAPTER 1

LITERATURE REVIEW

Variation in feelings towards surveillance

Since the dawn of digital surveillance, public sentiment towards surveillance has been varied. Anecdotally, this was demonstrated by responses to several recent changes in surveillance policy. In 2016, Facebook announced that despite initial reassurances, it would begin sharing user data between the WhatsApp and Facebook platforms (Tech Crunch, 2016). The changes meant that Facebook could aggregate user data from both platforms to infer their likes, attitudes, contacts, and behaviour. Whilst this prompted investigation from both the United Kingdom's (UK) Information Commissioner and the European Commission, the public appeared undaunted, as active users on WhatsApp increased from 500 million to 1.2 billion between 2015 and 2017 (Statistica, n.d.). In contrast, the British government was met with a public outcry after it proposed changes to the way it could access people's online data. In November 2016, the UK Houses of Parliament passed The Investigatory Powers Act 2016, which ruled that all website and phone companies must retain customer data for a minimum of 12 months. The new legislation would allow security services unrestricted access to companies' customer records and the ability to collect data from personal computers and mobile devices. The media soon dubbed the law 'the snoopers' charter' (Travis, 2016) and a petition to repeal the bill garnered over 200,000 signatures (Skillinger, 2016).

Variation in responses towards surveillance has also been demonstrated in public polls. A YouGov poll conducted in 2013 found that British people were largely divided on Government Communications Headquarters (GCHQ) mass

surveillance. When asked if they believed that GCHQ were right to conduct mass surveillance on people not suspected of wrongdoing, 41% believed that GCHQ were right, whereas 45% believed they were wrong. American polls have also demonstrated division in feelings towards surveillance; a small majority of 54% approved of NSA surveillance, whereas 42% disapproved (Gao, 2015).

Academic research presents a similar picture. Oulasvirta et al. (2012) measured participants emotions and feelings towards surveillance over a 6-month period whilst their homes were fitted with CCTV. It was anticipated that all participants would (at least initially) feel negatively about the surveillance, yet this was not the case. Whilst some participants felt hostility and even rage towards the surveillance, others reported more positive feelings, to the extent that they gave names to the cameras in their home. Similar results have also been found through focus groups. Pavone and Esposti (2010) found that some participants had few concerns and felt trusting of surveillance technologies, whilst others were intensely distrustful and felt surveillance jeopardised their privacy without improving security. In sum, society appears ambivalent towards surveillance, yet the processes that may contribute to this variation are poorly understood and rarely researched.

This thesis aims to address this gap in the literature by exploring the effects of surveillance *accuracy* (rather than simply comparing the effects of surveillance when it is present versus absent). Additionally, we examine potential positive psychological outcomes in the form of group-based recognition, as this may help explain why individuals feel less negatively or more positively towards surveillance in some circumstances.

The importance of understanding the processes that contribute to feelings towards surveillance

Considering the ubiquity of surveillance, it is vital to understand the processes that determine how people feel towards these technologies. Surveillance systems are embedded within modern society. They underpin much of our communication (Cohen, 2008), purchasing (Schneier, 2015), access to information and resources (Pariser, 2011; Vaidhyanathan, 2018; O'Neil, 2016), opportunities for education or employment (O'Neil, 2016), and political engagement (Vaidhyanathan, 2018). According to the former Google chief executive officer, Eric Schmidt, the future heralds an even greater assimilation between online and offline life: 'the internet will disappear. There will be so many IP addresses…so many devices, sensors, things that you are wearing, things that you are interacting with, that you won't even sense it. It will be part of your presence all the time' (Smith, 2015; para 2-3). Here, Schmidt implies that the internet will cease to exist as a platform on which you log in or log off. Instead it will become a constant, seamlessly operating in parallel to our daily life. Indeed, Lanier (2018) argued that surveillance is so ingrained within society that '…if two people wish to communicate the only way that can happen is if it's financed by a third person who wishes to manipulate them' (14:14).

As surveillance is so embedded in daily life, our feelings towards surveillance may have implications for how individuals and groups communicate, spend their money, and engage politically. In this thesis we do not suggest that surveillance is inherently good or bad, nor do we qualify the broader implications of surveillance. Instead we suggest that the research community and the wider public may only fully understand the implications of surveillance when the processes underlying society's feelings towards it are

better understood. Despite a general lack of research on these potential processes, several psychological outcomes have been highlighted in previous work – some of which serve the basis of this thesis. These include a lack of perceived control, chilling effects, privacy concern, and group-based recognition.[2]

Predictors of feelings towards surveillance

To date, the surveillance literature has highlighted several factors that predict how we feel towards surveillance. These factors are typically negative, in that those under surveillance are described as experiencing more negative psychological/behavioural outcomes than those not under surveillance. Here, we will turn our attention to the most prominent negative drivers of feelings towards surveillance highlighted in the literature thus far: a lack of perceived control, chilling effects, and privacy concern.

Negative psychological drivers. *Perceived control*. A sense of control is critical for wellbeing. For example, those who perceive more personal control are more likely to be happier (Larson, 1989; Verme, 2009) and report greater levels of wellbeing generally (Spector et al., 2002). Additionally, feeling *less* control is associated with various forms of psychological distress, such as depression and anxiety (Glass, McKnight, & Valdimarsdottir, 1993; Griffin, Fuhrer, Stansfeld, & Marmot, 2002). Understandably, then, individuals tend to favour environments which facilitate a sense of control and avoid those which diminish it. Indeed, those who feel less control at work are more likely to report low work satisfaction (Caprara, Barbaranelli, Steca, & Malone, 2006) and higher turnover rates (Jensen, Patel, & Messersmith, 2013). Consequently, individuals typically dislike and avoid stressors which diminish their sense of control.

[2] Privacy concern and group-based recognition are the focus of this thesis.

Historically, surveillance has been used as a method of controlling others. For example, surveillance can control where and when individuals gather together in public spaces, and more recently, whether certain groups are intercepted before travelling at airports (Blackwood, Hopkins, & Reicher, 2015). This dynamic of control also exists online. Surveillance algorithms often limit users' choice of content by using prior online behaviour to manipulate what we are shown in the future. Specifically, personalised material is designed to align with our inferred attitudes and beliefs, creating a cycle of attitude reinforcement known as a filter bubble (Bozdag & van den Hoven, 2015). As a result, filter bubbles reduce the diversity of content that users are exposed to and restricts access to content users would otherwise interact with. Indeed, Eslami et al. (2015) illustrated that Facebook users are shocked when they learn algorithms manipulate what content is shown on their news feed, with one participant drawing comparisons between the platform and a science fiction dystopia: '…it's kind of waking up in the Matrix in a way…you think about, kind of, how much control they have' (p. 6). Additionally, when given a choice of diverse content, users consume as much belief-affirming content as disaffirming content (Gladfelter, 2018). Therefore, surveilling algorithms often homogenise the content users are exposed to, which typically diverges from the unfiltered content users choose to consume.

As well as controlling the content we are exposed to, algorithmic surveillance diminishes the control we have over our own data. Individuals strive to maintain integrity (or contextual integrity – Nissenbaum, 2004) by managing the different facets of their identity depending on their audience. Goffman (1959) argued that we behave within the boundaries of norms dictated by our context – and our context is often defined by those around us (Davis &

Jurgenson, 2014). From this perspective, Goffman suggests we do not have a single identity, but multiple facets of self which we choose to express in some contexts and not others. This is also true of online contexts; our online personas are often extensions of our 'real' self, and we shape our behaviour in relation to our perceived audience (Miller, 2013). For example, Humphrey (2009) found that those in chat rooms express multiple identities depending on their position on the platform. One platform user changed their avatar in response to being criticised over their post; their new avatar communicated their perceived victim status to the others in the group.

Users can lose control over their performed identity when data becomes accessible to inappropriate or unexpected audiences (Garrido, 2015). This can occur online when organisations harvest and share our data with third parties. In these circumstances, users are prevented from managing their identities appropriately (Brown, 2013). This is known as context collapse (Wesch, 2009; Marwick & Boyd, 2011), whereby the boundaries between contexts becomes blurred. Users respond negatively towards this sort of loss of control over online data: Mamonov and Koufaris (2016) found individuals became concerned about surveillance when they believed their data were being shared with unknown third parties. This has also been demonstrated by Koskela and Tuominen (2003; cited in Koskela, 2004) who found that whilst people were accepting of CCTV surveillance in public spaces, they felt more negatively about the technology when they were told the footage would be used by the media for entertainment purposes. Consequently, surveillance can diminish our sense of control and can in turn make individuals feel more negatively towards surveillance systems.

Chilling effects. Our inability to control the flow of our data can lead to a further negative outcome of surveillance: chilling effects. This occurs when an individual modifies their behaviour or removes themselves entirely from an online context in response to surveillance (Marthews & Tucker, 2017; Penney, 2016; Stoycheff, 2016).[3] Foucault initially described this phenomenon as a social good; when reflecting on Bentham's panopticon design, Foucault suggests that surveillance serves as 'a gaze which each individual under its weight will end by interiorising to the point that he is his own overseer' (p. 155). Thus, an individual only needs to be aware of the *potential* for surveillance for it to exert psychological and behavioural pressures. In an online context, these individuals may be behaving in entirely lawful ways, yet the inability to control who has access to their online data or how this might be interpreted discourages innocent behaviour or involvement (Penney, 2016). Often, this originates from fear that state organisations will improperly use their data to justify punishment or discrimination (Penney, 2016).

The 'chilling' phenomenon was demonstrated by Marthews and Tucker (2017), who found that online search behaviour changed after the 2013 Snowdon revelations.[4] In their study, they found that people were less likely to search for sensitive terms after the revelations ('pipe-bomb' was considered highly sensitive) compared to before. Similarly, Penney (2016) found that controversial Wikipedia articles received less internet traffic after the Snowdon revelations. Together, this suggests that a loss of control over who is privy to our online data may encourage individuals to disengage or modify their

[3] Chilling effects operate as both a psychological and behavioural consequence of surveillance. Despite there being a behavioural component, we argue that chilling effects may also predict negative feelings towards surveillance. Arguably, individuals may be more likely to feel negatively towards surveillance if they feel surveillance has exerted psychological and behavioural pressures.

[4] Snowden was a former contractor for the Central Intelligence Agency (CIA) who exposed pervasive surveillance of US civilians by American intelligence in 2013.

behaviour online, which may in turn cause users to feel more negatively towards surveillance.

***Privacy concern*.** The negative outcomes described thus far do not appear in isolation but are often interrelated and experienced in tandem with one another as a general sense of concern (Ellis, Tucker, Harper, 2013; Penney, 2016). The most prominent concerns reported in the literature are those of safety and privacy (Ellis et al., 2013; Patel, 2012),[5] the latter being most discussed (Graham & Wood, 2003) and also central to this project.

Many definitions of privacy reinforce its connection with control; the object of control differs depending on the chosen definition (see Stuart, Bandara, & Levine (2019) for an overview). Altman (1975) defined privacy as 'an interpersonal boundary process by which a person or a group regulates interaction with others…involving selective control over a self-boundary' (p. 6). Whilst earlier conceptions of privacy focus on informational control (e.g. Westin, 1967), Altman's definition emphasises that privacy also involves interpersonal control; i.e., the management of who you or your group interact with. The notion of interpersonal control is also mirrored in Margulis' (1977) definition: 'privacy is an interpersonal boundary control process that regulates, paces, and controls social interaction' (p. 12). In an online context, control over interaction partners and personal data are inextricably linked. Who we interact with is registered as data currency and potentially shared with third parties. This data also feeds into who we are encouraged to interact with in the future (Hunt, 2016). Indeed, the multifaceted nature of privacy has been noted by others (Cho, Rivera-Sánchez, & Lim, 2009), in that privacy is the ability to control multiple aspects of one's life.

[5] It is worth noting that whilst some surveillance systems are designed to ostensibly improve safety, those who feel personally targeted often report less safety when under surveillance (Patel, 2012).

Reports of privacy concern are especially prominent during the implementation of new technologies with surveilling capabilities; when users are aware of surveilling components within a technology, privacy often becomes a salient concern (Möllers & Hälterlein, 2013). For example, Wang et al. (2014) found that when participants were aware of surveillance on social media, they reported more privacy concern and altered their behaviour to restrict access to their content. This has also been demonstrated by Almuhimedi et al. (2015), who notified participants when (and how much) data had been shared with third parties on their phone. When receiving these nudges, participants reported more concern about access to personal information – such as location data – and stated that apps running in the background on their phone made them feel 'followed' (p. 17). Participants were also more likely to restrict permissions on their phone when they were made aware of app access. More moderate levels of privacy concern are found when individuals are not directly informed about surveillance. For example, Paine, Reips, Stieger, Joinson, and Buchanan (2007) asked participants if they were concerned for their privacy whilst online, without reference to any specific surveillance technique. They found that only a modest majority (56%) of participants felt concerned for their privacy online. This suggests that when individuals are aware of surveillance, they are more likely to report privacy concerns and may be more likely to alter their privacy behaviours online (see also Khovanskaya, Baumer, Cosley, Voida, & Gay, 2013).

The privacy paradox. Despite this, others have argued that privacy concern rarely translates to behaviour change. Whilst individuals report concern for their privacy, they often do little online to protect it. This is known as the privacy paradox (Barnes, 2006; Norberg, Horne, & Horne, 2007). One of the

first illustrations of the paradox was provided by Spiekermann, Grossklags, and Berendt (2001). Participants were first asked about their privacy preferences and attitudes, including the information they would be willing to provide and how concerned they were in general about their personal data. They then introduced participants to a shopping platform which requested numerous aspects of personal information (e.g. how photogenic they believed themselves to be and their home address). The researchers found that the majority of participants were willing to disclose personal information when prompted, despite reporting concerns for their privacy online. The privacy paradox was also shown more recently by Athey, Catalini, and Tucker (2017), who found that when the disclosure of personal information is incentivised (through either reward or cost), participants are willing to relinquish personal data despite concerns for privacy. As a result, some have heralded the end of privacy (Preston, 2014), arguing that privacy concerns appear inconsequential when sharing has become the norm and organisations hoover up the wealth of information users provide.

Nevertheless, the presence of the privacy paradox has been questioned for numerous reasons. Firstly, many people may not perceive an alternative to disclosing their personal information online. Tene and Polonetsky (2014) argue that software and browser settings intended to help users control their data online are often too complex for the average internet user to navigate. The authors argue that this is especially true when surveillance technologies rapidly evolve in order to out-manoeuvre data protection services. This requires users to routinely update their software and settings. Some have even suggested that privacy settings and services may be purposefully obscure, as business models of platforms (such as Facebook) rely on disclosure (Brown, 2013). Therefore,

despite many users' best efforts, information disclosure is often unavoidable or even accidental.

Aside from the technological pressures to disclose information, social pressures may also limit users' perceived options for privacy control. Compliance with surveillance practices is viewed as necessary to achieve digital engagement (Obar & Oeldorf-Hirsch, 2018). This is especially true for social networks, which often require users to divulge personal information before creating an account. As many offline interactions now predominantly take place online, users risk social isolation if they are not willing to provide this data (Welinder, 2012). As a result, users become embedded within online networks and their ability to remove themselves – whilst maintaining social connectivity – relies on others in their network following suit (Welinder, 2012). Furthermore, social network platforms actively discourage user abandonment. Facebook presents those attempting to deactivate their account with pictures of their closest friends, warning them that these individuals will no longer be able to keep in touch once the user has left (Hoare, 2010).

The risk of social exclusion encourages users to be present, but to also actively engage with the platform. Normative pressures to disclose online were evidenced by Acquisti, John, and Loewenstein (2012). In their study, participants were asked sensitive questions about their engagement in unethical behaviours. After each question, participants were informed that either most or few people had provided an answer. The authors found that participants were more likely to divulge sensitive information if they believed others had also done so. Welinder (2012) described platforms that operate in this way as 'beautiful walled gardens' (p. 216), as users have little choice but to register and participate. Platforms are also not incentivised to change privacy policies, as

users are unlikely to abandon platforms (due to social costs) despite privacy concerns (Welinder, 2012). Therefore, information disclosure is often perceived to be the *only* choice for many users.

It is clear, then, that users experience multiple obstacles when attempting to maintain their online privacy. Nevertheless, these barriers continually shift as organisations adapt their privacy policies in response to public sentiment; this often reignites discussions surrounding privacy concern. In many circumstances, company surveillance policies have evolved to reflect users' needs, abilities, and demands (Möllers & Hälterlein, 2013). For example, in March 2019, Mark Zuckerberg announced that the company aimed to become more privacy focussed and promised that less metadata would be retained by the company (Newton, 2019). Additionally, data-sharing scandals ensure issues surrounding privacy remain at the forefront of public debate. In 2018 the public learned how a Facebook app allowed Cambridge Analytica to harvest data from 87 million Facebook profiles, which was subsequently used to influence both the EU referendum and the US presidential election (Chang, 2018). Additionally, a popular face modification app called 'FaceApp' was recently criticised for its data sharing practices, along with its potential ties to Russia.[6] As such, privacy is likely to remain a prominent concern for many users (Paine et al., 2007; Phelps, Nowak, & Ferrell, 2000), and society is likely to continue demanding greater data control. In light of this, developers may benefit from an increased understanding of when and why privacy becomes an issue for users, and in what circumstances users may benefit from greater privacy and control. As such, processes associated with user privacy concerns

[6] The app's data sharing practices are still considered questionable, however the app's ties with Russia have since been considered non-nefarious (Brewster, 2019).

remain a valuable avenue of research within surveillance studies. The current thesis examines the processes surrounding privacy online. In particular, we explore whether more accurate surveillance heightens privacy concern, and whether this in turn contributes to more negative (and less positive) feelings towards surveillance.

Privacy concern and feelings towards surveillance. As discussed, privacy concern can be a common outcome of surveillance. Perhaps unsurprisingly, qualitative research and anecdotal evidence have found greater concern for one's privacy is associated with increased negativity towards surveillance. Pavone and Esposti (2010) found that individuals with greater privacy concerns felt more negatively towards surveillance compared to individuals who did not feel as though surveillance was an invasion of privacy. Similarly, after installing a surveillance system in participants' homes, Oulasvirta and colleagues (2012) found that some participants reported a strong dislike towards the surveillance, as they became deeply concerned for their privacy.[7] On the other hand, participants who did not perceive the surveillance system as an invasion of privacy saw the system as a friendly entity, to the extent that some participants gave names to individual cameras. The association between privacy concern and feelings towards surveillance is further illustrated by the public's reaction to Facebook's creation of the 'News Feed'. In 2006, upon logging in, a user was presented with an aggregation of all their friends' recent activity (e.g. relationship status changes and befriending). Users became outraged and concerned that their information (although not previously private) became so easily accessible to others, and many users formed groups such as

[7] Privacy concerns typically related to participants' common daily activities, such as undressing or speaking on the telephone.

'Students Against Facebook News Feeds' in protest (boyd, 2008[8]). In sum, those with greater privacy concerns under surveillance are likely to experience more negative feelings towards surveillance and surveilling platforms compared to those who have fewer concerns for their privacy.

However, the direct relationship between privacy concerns and feelings towards surveillance has not explicitly been explored. Typically, this association has been implied through qualitative work. For example, a potential association between privacy concern and feelings towards surveillance was found by Pavone and Esposti (2010) through focus groups, as participants typically voiced negative feelings towards surveillance in conjunction with an experience of privacy concern. Additionally, *general* affect towards surveillance has rarely been explored. Previous research has either included privacy concern as the dependent variable (e.g. Alge, 2001; O'Donnell et al., 2010) or have explored other outcomes of privacy concern, such as willingness to share data online (Dinev, Hart, & Mullen, 2008). However, others have noted that surveillance can contribute towards a general feeling or affect. Ellis et al. (2013) argue that the multiplicity of psychological outcomes from surveillance creates an affective atmosphere, which is an abstract sense or impression of something – a general feeling. Ellis and colleagues argue that the general affective response to surveillance deserves more psychological research, as surveillance 'systems grow in stature and complexity' (p. 729). The authors argue that the affective response to surveillance can impact on how society relates with it. Therefore, we aim to empirically test whether feelings towards surveillance are in part predicted by privacy concern.

[8] dana boyd has requested that her first and last name be kept lower case (see www.danah.org/name for an explanation). As such, all references of dana boyd will not be capitalised in this thesis.

Positive psychological drivers of feelings towards surveillance.

There are clearly a number of negative psychological outcomes associated with online surveillance. However, in order to explain the variation in public reactions towards algorithmic surveillance we must also examine potential positive psychological outcomes. As of yet, this subject has not been explicitly investigated. Here, we suggest that recognition can be a positive outcome experienced by those surveilled online and may facilitate more positive (and/or less negative) feelings towards surveillance.

Recognition. Surveillance may foster a greater sense of recognition in some circumstances. Before outlining the evidence in support of this, it is important to define what is meant by recognition in this context. Typically, the concept of recognition is poorly understood, and recognition is rarely defined in literature (Bartelson, 2013). Our conceptualisation of recognition developed throughout this project, as we included (and in some cases later excluded) dimensions of recognition that had been suggested in previous work. Additionally, we explored recognition in both individual and group-based contexts, and the dimensions of recognition included here will be explored from both an individual and social identity perspective. We describe the four dimensions of recognition included in this thesis below.

Accuracy. Firstly, one must be seen accurately (i.e., as one intends to be perceived) in order to be recognised. Goffman (1956) argues that identity is multifaceted, and each facet of identity is more or less appropriate for a given context and audience. A ‘performer’ will choose which aspect of their identity to disclose to their audience, and which ones to hide. Ultimately, the performer hopes that the audience accepts this display as being an honest representation, and that they perceive the performer in the way intended. In other words, our

aim when interacting with others is that they develop an accurate impression of who we are. Whilst implied, Goffman does not explicitly state that identity performances are to foster social recognition, nor does he argue that accurate impressions constitute social recognition. However, others have argued that in return for our identity performances, we have a reasonable expectation for social recognition (Jacobsen & Kristiansen, 2015). Therefore, it may be argued that the accuracy of others' impressions of us are necessary for perceived recognition to occur.

The importance of impression accuracy is also described in self-verification theory (Swann & Read, 1981; Swann, Rentfrow, & Guinn, 2003). The theory suggests that individuals attempt to create accurate impressions of themselves in their interaction partners. In turn, individuals hope to receive feedback from others that corresponds to how they perceive themselves. This then validates the individual's own self-concept (i.e., thoughts and feelings about the self; Swann & Read, 1981). Arguably, the theory suggests that recognition – which ultimately fosters self-validation – is only possible if we believe others hold an accurate impression of our identity.

Indeed, the role of accuracy as a component of recognition – particularly online – is evidenced in previous research. For example, individuals often use online platforms to engage in identity performances (Kennedy, 2006). Kennedy (2006) interviewed women involved in the Her@ project, an initiative to help disadvantaged women gain access to higher education through computer-mediated distance learning. In this project, women were asked to create homepages of themselves. One participant highlighted how it was important for her to accurately represent herself on her homepage in order to be recognised by her peers: 'I felt it was difficult to incorporate the 'right' image of myself, an

image I wanted the rest of the world to see and like' (p. 12). Similar sentiments were found in young girls using social media. Steeves and Bailey (2016) interviewed young female Facebook users, who explained that an accurate profile was integral for facilitating recognition from their peers; they described how Facebook allowed them to 'build a picture of themselves as what they want to be perceived as' (p. 6); 'you just want people to associate the face that you kind of posted on Facebook with who you are' (p. 7). The participants also voiced concern over being seen inaccurately; users were afraid of 'being perceived as something I'm not' (p. 12). This suggests that an accurate representation online is a key component of recognition from others.

Other notable work has also considered accuracy to be central to the conceptualisation of recognition. For example, Hopkins (2011) conceptualised recognition as the acknowledgment of one's group membership. Through interviews, Hopkins (2011) found that participants experienced recognition when their dual identities were accurately identified by others; one participant felt recognised when her friend commented that her dress sense embodied both her British and Muslim identity, 'I love this urban Muslim female look because you are marrying the Britishness with your Islamicness' (p. 266). In this case, to be recognised is to be accurately identified as a member of your group(s).

Conversely, individuals experience *mis*recognition when they believe others perceive them inaccurately. This is commonly illustrated in categorisation threat or identity denial research, whereby individuals are mistakenly assumed to be a member of another social group, or to not belong to the group to which they identify. For example, in Hopkins and Greenwood's (2013) research, Muslim participants explained that others would often assume that they were foreign from their Muslim dress (e.g., the hijab). Similarly, Blackwood, Hopkins,

and Reicher (2013) interviewed British Muslims about their experiences at airports and found that participants reported frequent miscategorisation as terrorists because of their Muslim identity: ‘when she goes travelling she takes the niqab off…because she knows people look at her like, yeah OK, she’s the scary one’ (p. 157). Indeed, the conflation of their Muslim identity with terrorism fostered feelings of misrecognition amongst many of the participants. In sum, this illustrates that accuracy (of others’ perceptions) is a fundamental dimension of recognition, in that recognition is in part experienced by being perceived accurately.

Distinctiveness. Identity is often considered a relational concept; identities do not exist in isolation but are instead defined by their position amongst others (Oyserman, 2004; Skeggs, 1999). As such, identity is conceived by how we are different (or distinct) from those we do not identify with. This is a central component of the social identity theory (SIT; Tajfel & Turner, 1979), which posits that individuals strive for their group to be seen as positively distinct from other groups. Differences between the ingroup and the outgroup are often exaggerated in order to emphasise group distinctiveness (Greene, 2004; Graham, Nosek, & Haidt, 2012). Consequently, we argue that being perceived as distinct is an important aspect of being recognised.

Individuals often experience distinctiveness threat (a form of identity threat) when others do not recognise their social identity as sufficiently distinct from comparison groups (Branscombe, Ellemers, Spears, & Doosje, 1999). When threat is experienced, individuals will often attempt to exaggerate distinctive group characteristics or intergroup differences to achieve recognition of their desired identity (the reactive distinctiveness hypothesis; Jetten, Spears, & Postmes, 2004). Individuals are even willing to incur personal costs in order

to maximise intergroup differences (Turner, Brown, & Tajfel, 1979). The preference for distinctiveness has also been found at the individual level. For example, Berger and Heath (2007) found that consumers who believed they were similar to the majority (e.g., in terms of preferences towards music and car brands) abandoned previously-stated preferences. Participants were also more likely to choose a product if it was the least-commonly chosen, unless this product was commonly chosen by an outgroup. Therefore, the authors argue that product selection was a strategy to ensure both individual and group-based recognition.[9] In sum, identity distinctiveness may be an essential component of identity recognition.

Positivity. Alongside distinctiveness, SIT also suggests that individuals strive for their identities to be perceived positively; often, groups do not simply want to be seen as different, they want to be seen *positively* relative to others (referred to as positive distinctiveness). Individuals will often enhance the ingroup (e.g., through ingroup favouritism) to maximise positive distinctiveness (Brewer, 1979). For example, in minimal group settings, individuals are more likely to rate their ingroup more favourably on important dimensions (Mummendey, 1984). The need to be seen positively is also supported in an online context by Steeves and Bailey (2016), who found that young girls online wanted to be seen as popular and attractive through their Facebook profile. One participant likened Facebook to "…a personal ad, yourself. Like, 'I'm a good time; if you're with me, you're going to have fun'" (p. 8). British Muslims have also expressed that being seen as different is often not enough to foster recognition; Hopkins (2011) found that although Muslims occasionally felt non-

[9] The phenomenon whereby individuals are motivated to achieve individual distinctiveness whilst maintaining group membership is known as Optimal Distinctiveness Theory (Brewer, 1991).

Muslims acknowledged their British-Muslim identity, the identity and culture was not always seen favourably: ‘I think the nation has to begin to see the achievements of the Muslim community. I mean we’ve put up some magnificent buildings’, “people should recognise this, ‘hey hang on, you guys are doing something’” (p. 263-264). Together, this suggests that individuals need to be seen as different, but also different in a *good* way in order to feel recognised.

Understanding. Whilst conceptually ambiguous (Reis, Lemay Jr, & Finkenauer, 2017), the final dimension of recognition encompasses and extends the aforementioned components. In addition to being perceived accurately, as distinct, and positively, the broader context of their identity must also be *understood*. Reis et al. (2017) describes felt understanding as when a “person ‘gets them’ in some fundamental way, and they tend to feel psychologically connected to this person” (p. 1). Understanding is a purposefully broad term, as it encompasses knowing the self; it is the knowledge of all expects and experiences that may comprise the self (Reis et al., 2017). For example, a transgender person may be accurately perceived by others as the gender they identify, they may be seen as distinct from other LGBTQ+ groups, and those around them may regard transgender people positively. However, others may not truly appreciate how important their identity is to them, or the struggles that they may experience. Here, we argue that this deeper level of appraisal is an example of understanding, which is considered a basic need from social interaction (Cahn, 1990).

Intergroup understanding has previously been encouraged to foster better intergroup relationships. For example, greater understanding has been found to predict more intergroup trust and forgiveness (Livingstone, Fernández Rodríguez, & Rothers, in press). Interventions aiming to improve intergroup

understanding have also had positive consequences for social relationships. Nagda, Gurin, Sorensen, and Zúñiga (2009) aimed to improve intergroup understanding by 'helping students explore their own and others' social identities and statuses, and the role of social structure in relationships of privilege and inequality' (p. 2). Indeed, understanding is considered integral for wellbeing (Lun, Kesebir, & Oishi, 2008) and relationship quality (Cohen, Schulz, Weiss, & Waldinger, 2012). Together, this may suggest that understanding is a further component of recognition, as it represents a deeper awareness of an individual or group's experiences and beliefs, which are integral to their identity.

The importance of recognition. The importance of recognition has been widely explored within philosophy literature. The most prominent theories of recognition have been proposed by Taylor (1994), Fraser (1995), and Honneth (1995). Each argue that identity is formed through social processes, and that recognition is borne from these social relations. They also highlight that recognition is fundamental for wellbeing; it is integral to develop 'a healthy and intact sense of self' and that this is 'a crucial ingredient of the good for individuals' (p. 519; Zurn, 2003). This is largely because we view ourselves through the lens of our society, as Laitinen (2003) argues: 'self-esteem depends on social esteem, self-respect on respect, basic self-confidence on love and care, self-consciousness on communicative treatment, self-images on others' views' (p. 2). In sum, how we see ourselves is largely dependent on how others perceive us. This can have profound consequences for our emotional wellbeing. If one's group is loved, then one may love themselves – if not, individuals may experience negative self-directed affect, such as self-loathing (Laitinen, 2003).

This is also supported by psychological evidence. Higher levels of recognition are associated with greater wellbeing (Oishi, Krochik, & Akimoto,

2010), autonomy (Renger, Renger, Miché, & Simon, 2017), self-esteem (Howarth, 2002; Shechtman & Bar-el, 1994), and relationship satisfaction (Murray, Holmes, Bellavia, Griffin, & Dolderman, 2002). Feeling recognised by others can also improve how individuals interact and feel towards those around them. For example, Simon and Grabow (2014) found that gay men who felt recognised within society had lower levels of anti-Muslim attitudes, suggesting that recognition not only improves how individuals feel about themselves, but also those around them.

Conversely, a lack of recognition can have deleterious effects. Bachmann and Simon (2014) found that gay men who did not feel recognised by society experienced poorer life satisfaction than those with greater levels of recognition. Misrecognition has also been associated with social isolation (McLean, 2008) and social pain; Morelli, Torre, and Eisenberger (2014) found that feeling misunderstood activated brain regions associated with social disconnection and negative affect, which are experienced similarly to physical pain. In sum, recognition is vital for developing a positive relationship with both the self and others. Given the intrinsic value of recognition, we suggest that recognition may partially explain the variation in feelings towards surveillance. As recognition is experienced positively, recognition from surveillance may encourage more positive and less negative feelings towards surveillance systems.

Surveillance and recognition. As discussed, algorithmic surveillance attempts to learn as much as possible about our identity from our online behaviour. We also receive feedback on the assumptions made about us, typically through online advertising. This gives internet users the unique opportunity to receive insight into how others perceive them and the groups to

which they belong. In turn, this may provide internet users with the opportunity for recognition; if surveillance feedback mirrors how individuals see themselves, they may feel better recognised. Indeed, surveillance has been shown to foster recognition in some surveillance contexts, namely social-veillance scenarios.[10] For example, Albrechtslund (2008) argues that social media gives users the opportunity to construct and communicate their identity on their own terms. In this context, surveillance through social media is a mutual exercise that can empower the user, as users can find online spaces where their desired identity is acknowledged by others. Supporting this, de Laat (2008) interviewed those using online platforms such as blogs, and found that users commonly expressed social recognition as a positive outcome from online engagement: "And to finally know that people out there actually did read what I had to say…'OK, what you are doing is good and you should keep on doing it'" (p. 62). This was also reported by an interviewee in Steeves and Bailey (2016), who noted that users '…are seeking that attention more, and seeking that approval' (p. 15).

Social-veillance also provides users the opportunity to achieve recognition after experiencing identity threat. Toma and Hancock (2013) found that participants were more likely to gravitate towards their Facebook profile after receiving negative feedback compared to those who had received positive feedback. The authors argued that their profile served as a venue for others to see them in their preferred state, therefore boosting recognition at a time of threat. Consequently, surveillance online may provide a vehicle for identity recognition in some contexts.

[10] Social-veillance (also referred to as lateral surveillance; Andrejevic, 2005, or participatory surveillance; Albrechtslund, 2008) is a term used to describe a scenario where the majority watch one another, typically via social media (Lupton, 2014). Social-veillance does not usually involve hierarchical differences between the surveiller and surveilled.

Group-based recognition in online contexts: The SIDE model. The majority of previous studies examining the role of recognition in online contexts typically focus on individual-based recognition. Studies often focus on the individual's personal online homepage, blog, or profile, and social identity (or group membership) is rarely referenced. Consequently, processes surrounding group-based recognition online is less understood. It is especially prudent to address this gap considering group-based processes may be especially pronounced in online contexts. The social identity model of deindividuation (SIDE; Lea & Spears, 1991; Reicher, Spears, & Postmes, 1995) suggests that group contexts or situations that render an individual anonymous make individualistic conceptions of the self less salient and instead heighten the salience of relevant social identities. Computer-mediated communication (CMC) arguably facilitates more anonymous communication, as individual identity cues may be less salient than face-to-face interaction (Dubrovsky, Kiesler, & Sethna, 1991). As a result, CMC obscures interpersonal differences, which in turn makes broader group characteristics more prominent.

This phenomenon was demonstrated by Postmes and Spears (2002), who found that men rated themselves as more masculine (compared to the self-reports of women) in anonymous CMC than men who were not anonymous. Additionally, men were more likely to display autonomous behaviour than women when anonymous in CMC. Furthermore, the anonymity offered by online contexts may embolden group normative behaviour; when using CMC, individuals are more likely to express group normative views punishable by an outgroup (Spears, Lea, Corneliussen, Postmes, & Harr, 2002). Together this suggests that online contexts may reduce the salience of interpersonal differences and heighten social identity, which has consequences for both

users' perceptions (e.g., increased stereotyping) and behaviour (e.g., increased stereotypical/group normative behaviour).

As social identity may have greater salience in online contexts, individuals may demonstrate greater sensitivity to opportunities online that foster group-based recognition and those that thwart it. The opportunity for recognition (or the risk of identity threat) may also depend on the perceived audience in online contexts. As argued by Klein, Spears, and Reicher (2007), whether the audience is considered an ingroup or outgroup determines the constraints in which identity is performed. Consequently, this thesis builds upon social-veillance literature that predominantly explores individual-based recognition in online contexts. From the perspective of the SIDE model, this thesis examines *group*-based recognition online. Specifically, in Chapter 3 we investigate group-based recognition online when the group membership of the surveiller is known. Intergroup processes associated with online surveillance is discussed in greater depth in Chapter 3.

Recognition and feelings towards surveillance. As a consequence of greater recognition online, individuals may feel more positively towards online surveillance systems. For example, internet users typically prefer online advertising when adverts appear to recognise their interests (Campbell & Wright, 2008; McDonald & Cranor, 2010). Additionally, Ur, Leon, Cranor, Shay, and Wang (2012) found that a subset of their participants implied that targeted adverts had an intrinsic value, irrespective of their utility (e.g. discounts and vouchers). Together, this suggests that when users believe their identity is recognised (from the content of targeted adverts) they may feel more positively towards surveillance.

The role of surveillance accuracy

Thus far, it has been suggested that both privacy concerns and recognition are key contributors to how individuals feel towards surveillance. However, we suggest that the levels of privacy concern and recognition depend on the accuracy of the surveillance; how we feel is determined by the extent to which surveillance gets us *right.* Here, our conceptualisation of surveillance accuracy pertains to the perspective of those surveilled. As proposed by SCT, individuals have multiple social identities, which vary in salience depending on the context. Social identity is therefore a fluid, rather than static, component of the self. From this, we define surveillance accuracy is the extent to which surveillance mirrors/captures how an individual defines themselves in that moment, including group-based self-definition or social identity. In other words, surveillance accuracy as we define it is in the eye of the surveilled. In this sense, social identity (or identity more broadly) is not a static trait to be inferred from an objective and stable quality of a person (e.g., Pham, Tran, & Hoang, 2019). Rather, surveillance accuracy as we define it relates to the subjective experience of the user, in terms of the degree to which surveillance (and its feedback) mirrors the users' own self-perceptions.

To date, the literature has typically assessed how individuals feel towards the presence (vs. absence) of surveillance (e.g. Blackwood et al., 2015; Dawson, Burnett, & McArdle, 2005; Marthews & Tucker, 2017; McDonald & Cranor, 2010; Oulasvirta et al., 2012; Pavone & Esposti, 2010). However, this thesis aims to take a more nuanced approach to better understand variation in feelings towards surveillance. Arguably, modern surveillance is more often present than it is absent. For example, in 2015 Julian Assange warned that 'we've increasingly become accepting of the surveillance that exists at all levels

of society. It's hard to escape from that in any traditional way' (Lee, 2015, para. 4). Furthermore, most individuals are aware (at least to some degree) of government surveillance practices following the Snowdon revelations (87%; Shelton et al., 2015). As such, it may be more fruitful to explore how individuals experience the nuances of surveillance. In particular, this project will focus on the role of perceived surveillance accuracy.

Surveillance accuracy can vary greatly. For example, those within the field of surveillance have suggested that the wealth of information collected can contribute to 'analysis paralysis' (para. 2), whereby too much information creates an excess of noise that can increase the likelihood of an error (Maass, 2015). Users are also aware of the variation in surveillance accuracy. For example, Ur et al. (2012) found that some participants enjoyed online surveillance when it offered a lower price for products that they had previously searched. Yet they also perceived inaccurate surveillance: 'I feel that sometimes advertisers stereotype me. I find this to be offensive…it's collecting all this information about you that doesn't even describe who you are' (p. 6). It is evident then, that modern surveillance can vary considerably in its accuracy and that users are aware of this variability. Therefore, the potential effect of surveillance accuracy on feelings towards surveillance and the aforementioned psychological outcomes will now be discussed.

Surveillance of greater accuracy may increase perceived recognition. Surveillance may enhance feelings of identity recognition in some contexts; however, it may be that users only experience greater recognition when surveillance is *accurate*. Users are more likely to report feelings of recognition from surveillance when targeted adverts accurately reflect aspects of their identity (Campbell & Wright, 2008; McDonald & Cranor, 2010). Those

online have also been shown to curate more accurate profiles in order to mitigate misrecognition; one participant in Marwick (2012) stated that ‘if there’s a rumour they can confirm or deny it on there’, suggesting that users can harness social media to create accurate impressions of themselves. These sentiments were also mirrored by participants in Steeves and Bailey (2016), who reported that social media allowed them to ‘build a picture of themselves as what they want to be perceived’ (p. 6). Thus, users strive for accurate profiles online to facilitate recognition from their peers.

On the other hand, users are also likely to report misrecognition (or less recognition) when surveillance is perceived as inaccurate. For example, Asian or Black individuals who do not identify as Muslim have reported feelings of misrecognition when they are mistaken as Muslim or a terrorist (Hopkins, Boteerill, Sanghera, & Arshad, 2017). Misrecognition has also been experienced by lesbians who do not adhere to group stereotypes; Tayor (2007) found that some lesbians were frequently misidentified as straight because they had ‘long hair’ and did not wear a ‘big leather jacket’ (p. 171). Participants reported that others’ inaccurate perceptions contributed to feelings of misrecognition and social exclusion. In sum, individuals are more likely to report feelings of recognition when they are perceived accurately and are less likely to report feelings of recognition when they are perceived inaccurately. As such, surveillance at greater levels of accuracy may facilitate identity recognition compared to surveillance that is less accurate.

Surveillance accuracy and privacy concerns. However, whilst accurate surveillance may encourage positive psychological outcomes (recognition), it may also contribute to greater privacy concerns. This was illustrated by a participant in Ur et al (2012), who felt uncomfortable about

targeted advertising because it appeared highly accurate: '…I notice that when I look at an email, the ad at the top seems to cater to what I'm looking at, and I just think that might be an invasion of privacy.' (p. 5). Those with greater privacy concerns are also more likely to fabricate personal details to decrease the accuracy of surveillance, suggesting that when surveillance is less accurate, privacy concerns are assuaged (Wirtz, Lwin, & Williams, 2007). Similar techniques have been developed to enhance privacy whilst under video surveillance. A method known as 'warping' uses an algorithm to obscure the faces of those surveilled; this method aims to increase privacy by making surveillance less accurate (Korshunov & Ebrahimi, 2013). Indeed, technology manufacturers have injected accuracy-limiting software into their apps or services to reduce privacy concerns in those using their products (e.g., reducing location tracking accuracy; Xu & Teo, 2004). Consequently, this suggests that accurate surveillance can increase privacy concerns in those surveilled, whereas less accurate surveillance is associated with fewer privacy concerns.

The present research

In sum, there is little research that addresses the broad variation in people's feelings towards algorithmic surveillance. This thesis addresses this gap in three ways: first, we go beyond the distinction of surveillance as either present or absent by examining the outcomes of perceived surveillance *accuracy.* Second, we build upon previous literature by examining both negative *and* positive psychological outcomes of surveillance. Lastly, whilst previous literature has focussed on individualistic psychological outcomes, we explore the social identity processes associated with surveillance. By building upon previous literature in this way, we argue that a more comprehensive and

nuanced perspective may be achieved, which can elucidate the processes predicting feelings towards surveillance.

In more concrete terms, we investigated whether variation in feelings towards surveillance may be partially explained by variation in perceived surveillance accuracy, and whether two countervailing pathways predict feelings towards surveillance: a negative pathway through privacy concerns, and a positive pathway through recognition (see Figure 1).

Chapter 2 reports our first study that tests this model in a general population. We manipulated surveillance accuracy and measured recognition, privacy concern, and feelings towards surveillance. In this study we did not make a social identity salient and did not specifically examine group processes in response to surveillance. Chapters 3-5 then report tests of the effects of surveillance accuracy within a social identity framework.

Chapter 3 tests the predicted model (Figure 1) within an intergroup context. Both surveillance accuracy and surveiller identity (ingroup vs outgroup) were manipulated. In this chapter we tested whether surveiller identity would moderate the relationship between surveillance accuracy and recognition, as the identity of the surveiller would determine recognition needs. Specifically, we predicted that no association would be found between surveillance accuracy and group-based recognition when the surveiller belonged to the ingroup, as recognition needs were already met. In this instance accurate surveillance may not provide any further recognition benefits. On the other hand, we predicted that outgroup surveillance would produce a linear effect of surveillance accuracy on group-based recognition, as the outgroup is typically assumed to misrecognise the ingroup, and therefore accurate surveillance serves as a vehicle for intergroup recognition.

Chapter 4 then reports tests of the predicted model within chronically-misrecognised populations. We suggested that the effect of surveillance accuracy on recognition would be especially pronounced in chronically-misrecognised groups, as group recognition needs are not met; therefore, accurate surveillance provides the opportunity for greater group-based recognition. As such, we predicted that findings from these studies would mirror those from *outgroup* surveillance in Chapter 3.

In Chapters 3 and 4 we suggest that accurate surveillance may facilitate group-based recognition for those chronically misrecognised or surveilled by an outgroup because recognition needs are salient. Chapter 5 then reports a test of this proposition by manipulating chronic (mis)recognition directly. Participants were informed that their group was either recognised or misrecognised by wider society. Surveillance accuracy was also manipulated. We predicted that surveillance accuracy would have a stronger effect on group-based recognition if participants believed that their group was chronically-misrecognised. Lastly, Chapter 6 provides a discussion of the findings from the empirical chapters and offers limitations and directions for future research.

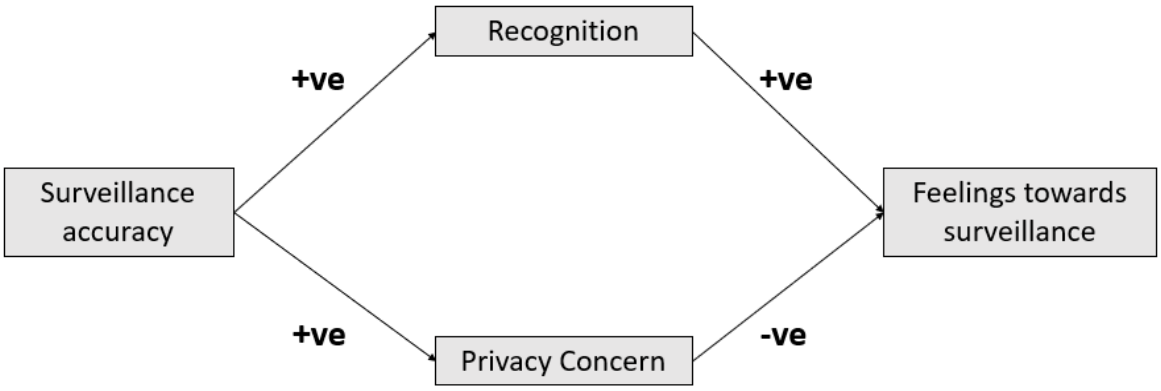


Figure 1. Theoretical model demonstrating the positive and negative pathway which produce countervailing effects on feelings towards surveillance.

CHAPTER 2

STUDY 1

Study 1 aimed to test the model outlined in Chapter 1 by manipulating the perceived accuracy of algorithmic surveillance, and examining its effects on feelings towards surveillance, on privacy concern and on recognition. To manipulate surveillance accuracy, participants were presented with an article ostensibly from *Wired* created by the researchers. In the article, surveillance was described as being of either low, medium, or high accuracy. Outcome variables were then measured using a survey.

Visibility

In Chapter 1 we outlined four possible dimensions of recognition: accuracy, distinctiveness, positivity, and understanding. Here we also suggest that all four dimensions rely on visibility. Consequently, an additional aim of this first study was to test whether visibility functioned as an additional positive driver of feelings towards surveillance (i.e., whether more accurate surveillance predicted more visibility, and whether this in turn predicted more positive feelings towards surveillance).

Visibility and recognition are related but distinct in important ways. Visibility is necessary – yet not always sufficient – to foster recognition. As Brighenti (2007) argues, recognition is not an inevitable outcome of visibility; individuals may be visible, yet they may also be *mis*recognised. Therefore, visibility may facilitate or obstruct recognition. Although there has been no direct examination of the link between surveillance accuracy and perceived visibility, research on social visibility amongst minority populations provides tangential evidence. Typically, groups that believe they are inaccurately perceived also

report feeling socially invisible (Clark & Griffin, 2008). In these cases, others' inaccurate perceptions involve a denouncement or denial of core components of their identity, which ultimately contributes to a feeling that their social presence is diminished.

Surveillance accuracy and visibility. The validation and worth of one's identity also rely on the perceptions of others (Fischer & Holz, 2007; Verkuyten, 2006); if society perceives an inaccurate version of oneself, the 'true' version of self is assumed less visible. For example, Clarke and Griffin (2008) interviewed older women about beauty and social visibility. While many participants felt physically visible, the inaccurate perceptions believed to be held by others (e.g., that older women lacked beauty and femininity) made them feel less socially visible: 'we won't love women if they're not lovely…for women who are older, we're invisible anyway' (p. 660). Additionally, racial minorities have reported feelings of social invisibility from others' inaccurate perceptions. In the context of a national celebration (a St Patrick's Day parade in Ireland), many ethnic minority individuals reported feeling as though their identity was invisible because of inaccurate or obscure representations of their identity in the parade: "here, you had people I think really wondering 'who the hell are these guys'" (p. 9; Pehrson, Stevenson, & Muldoon, 2014). Consequently, it could be argued that as surveillance becomes more accurate, individuals are more likely to feel visible.

Visibility and feelings towards surveillance. In turn, the more visible individuals feel, the more positive they may feel towards surveillance, as visibility enables the self to have a social presence. Supporting this, individuals are often drawn to and feel more positively about media which grant them greater visibility (McGrath, 2004). Likewise, Bucher (2012) argues that

Facebook offers the promise of visibility, but also the threat of invisibility if a users' content is not favoured and thus promoted by a platform's algorithms. As a result, individuals are motivated to participate on Facebook to gain visibility and avoid potential social invisibility. Furthermore, Steeves and Bailey (2016) found that young girls felt favourably towards Facebook because it provided them with visibility within their social network. As a result, greater perceived visibility from surveillance is likely to predict more positive feelings towards surveillance. Therefore, whilst conceptually distinct, we predict that visibility and recognition are both positive psychological outcomes of surveillance accuracy (Figure 2).

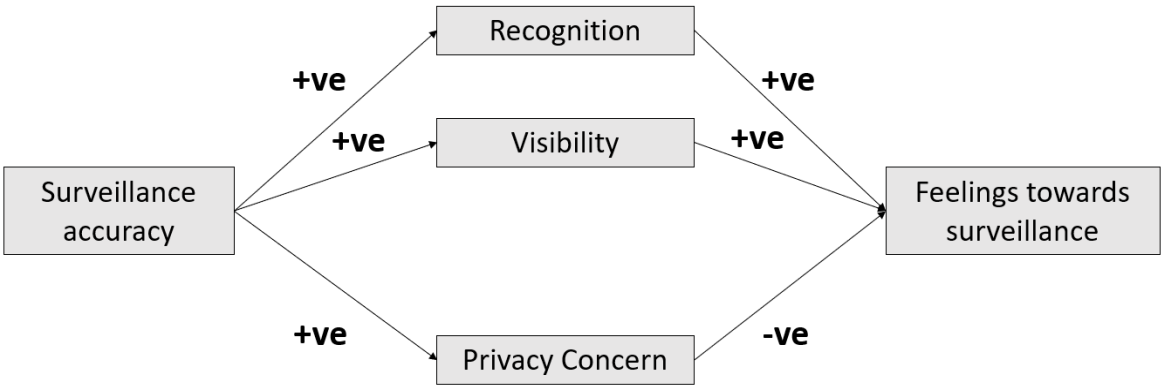


Figure 2. Predicted model with visibility as an additional mediator.

Method

Participants and design

Opportunistic sampling was used to collect data from 152 participants. Recruitment predominantly took place on university grounds and included both staff and students. Online recruitment also took place using platforms such as Facebook and Twitter. Respondents were aged between 19 and 72 years (M = 34.29, SD = 15.79) and 53% were female (44% were male, 1% chose not to

indicate their gender and 2% did not provide a response). The majority of participants were British (82%) with the remaining participants holding other European nationalities (7%) or nationalities from outside of Europe (including Indian, Brazilian and Canadian nationalities; 6%). The remaining 1% did not provide a response. Participants held a variety of occupations; 30% were students, 55% were employed, 1% were homemakers, 7% were unemployed and 7% did not wish to provide an answer or did not respond.

A sensitivity analysis using g*power indicated that the sample of the current study is sufficient to detect an effect size using ANOVA of $f = 0.25$ ($\eta_p^2 = .06$) with 80% power for the main effect of surveillance accuracy ($df_{num} = 2$). When using regression (three predictors), the current study is sufficient to detect an effect size of $f = 0.23$ (partial $r = .22$) with 80% power for each of the effects of recognition, privacy concern, and visibility.

The study had a one-way experimental design. Accuracy of surveillance was manipulated as a between-participant factor to create three levels: low, medium, and high (Appendix A). The dependent variable was participants' feelings towards surveillance. Mediators included privacy concern, perceived recognition, and visibility. While not explicitly hypothesised, we also reasoned that the amount an individual used the internet may affect the relationship between surveillance accuracy and psychological outcomes, as internet use has previously been shown to have a moderating effect on other online behaviour (Wilkins, Livingstone, & Levine, 2017). In this study, it is possible that the accuracy of surveillance may be more relevant for those who spend more time online compared to those who do not. For the latter, they may engage in less identity-relevant behaviours online and thus the accuracy of surveillance may have less of an effect. Consequently, the amount participants spent on the

internet was included as a potential moderator for follow-up analyses. A number of exploratory dependent variables and moderators were also included in the survey but are not discussed in the results of this report as they are not relevant to the hypotheses described above. A full list of the measures may be found in Appendix B.

Measures

Unless otherwise stated, responses to each item were recorded on a 7-point scale (1 = *Strongly disagree* to 7 = *Strongly agree*).

Manipulation. Participants were initially presented with a fabricated article ostensibly from the media source *Wired,* titled 'Our digital footprint: are algorithms any good at tracking us online?'. There were three versions of the article (one for each condition), and each contained a version of the accuracy manipulation text. In all conditions the article explained how we leave a digital trace online, which can be harvested by both private and state organisations. It also highlighted that the purpose of surveillance was to make predictions about internet users and their behaviour. Following this, the accuracy of surveillance was manipulated. The low accuracy condition informed participants that their data profiles produced by algorithmic surveillance were 19% accurate. In the medium accuracy condition these profiles were described as 50% accurate, and in the high accuracy condition they were described as 81% accurate.

Manipulation check. Six items were included to ensure that participants' perceptions of surveillance accuracy corresponded to their assigned condition. Items included 'In my view, algorithmic surveillance is accurate in identifying people'. On analysis items 5 and 6 did not conceptually relate to accuracy so much as the scope or extent of surveillance ('…able to access many aspects of people's lives', '…limited in what types of information it can gather on people'),

and did not correlate well with the other items. Additionally, the negatively-phrased items did not load onto the same factor as positively-phrased items. Therefore, the negatively-phrased items along with items 5 and 6 were deleted and the remaining positively-phrased items (items 1 and 3) were averaged to create the manipulation check scale *(r* = .46, *p* < .001; *M* = 4.20; *SD* = 1.19).

Feelings towards surveillance. Semantic differential scales were used to measure participants' emotional response towards algorithmic surveillance. Negative adjectives were placed at the left-hand side of the scale and their positive antonyms were listed to the right (e.g., worried/calm; uncomfortable/comfortable; annoyed/pleased). Participants were asked to place a tick on one of the 8 points along the (unnumbered) scale to represent which adjective best described their feelings. On review, the adjective pairs repressed/free and powerless/in control did not conceptually align with the other adjective pairs and were dropped from the scale. Additionally, disinterested/engaged did not correlate well with the other items. As a result, the scores for the remaining seven pairs were averaged to create the feelings towards surveillance scale (α = .93; *M* = 3.42; *SD* = 1.24).

Visibility. Six semantic differential items were used to assess how visible participants felt in response to algorithmic surveillance (e.g., visible/invisible; identifiable/anonymous; known/unknown). The scale consisted of 8 unnumbered points between each adjective. Two adjective pairs (misrepresented/understood and judged/unappraised) did not correlate well with the other adjective pairs. On reflection, these items referred to a process subsequent to becoming visible, rather than visibility per se. As a result, these two pairs were removed and scores on the remaining four items were averaged to create the visibility scale (α = .83; *M* = 2.60; *SD* = 1.05).

Privacy concerns. Four items measured how concerned participants were for their privacy due to algorithmic surveillance (α = .71; *M* = 5.00; *SD* = 1.14), for example 'internet surveillance is an invasion of privacy' and 'internet users have a right to use the internet without being surveilled'.

Recognition. Six items measured the extent to which participants felt recognised. Two items related to the sub-dimension *accuracy* (e.g. 'algorithmic surveillance can accurately portray everything about me'), two items related to the dimension *distinctiveness* (e.g. 'algorithmic surveillance can accurately distinguish me from others'), and two items related to the *understanding* sub-dimension (e.g. 'someone using algorithmic surveillance could know me better than I know myself'). Scores were averaged to create the recognition scale (α = .78; *M* = 3.02; *SD* = 0.99).[11]

Demographics. ***Internet use.*** The amount of time participants spent online was measured by asking participants to estimate the number of hours per week they spent on the internet. This was measured with an open response.[12]

Personal information. Age, gender, nationality, and occupation were requested, and responses were given in open-ended format.

Procedure

Paper-copy survey. Participants were approached in person primarily on University grounds. Participants were told that the survey concerned people's attitudes towards online surveillance. It was explained that an article from a technology magazine was included to ensure participants understood the

[11] Other items were initially included in the recognition scale but were not included in the analyses due to poor conceptual fit. These included those relating to discrimination (a process following *mis*recognition, e.g. 'internet users could be treated unfairly because of algorithmic surveillance') and perceptions of scrutiny (e.g. the use of algorithmic surveillance makes me feel analysed').

[12] Participants were also asked to estimate how many minutes they spent online in a single session, however this was not used in the analyses as hours per week was considered a more comprehensive measure of time spent online.

nature of algorithmic surveillance before participating. Once a consent form was signed, participants were given the stimulus article (Appendix A) and the survey. On completion, participants were thanked for their participation and were offered a debrief sheet which explained the details of the study and outlined the accuracy manipulation. They were assured that the article and the information within the text were not genuine. Participants were also provided with various online sources regarding data privacy, should they have any concerns or want to know more about the topic.

Online survey. Recruitment online occurred through snowball sampling. A link to the online survey was posted on a variety of Facebook groups accessible to the primary researcher. The researcher also requested that others share the link on their Facebook profiles. A similar approach was taken via email, whereby the researcher emailed personal contacts and requested their participation. They were also asked to email the link to others within their contact list. On opening the link, the participants were presented with a consent page. Once consent was given, participants were randomly assigned to one of the three versions of the *Wired* article. The materials presented in the online version were identical to those provided during paper-copy recruitment.

Results

Manipulation checks

There was a significant effect of condition (accuracy) on perceived accuracy of surveillance, $F(2, 149) = 14.49$, $p < .001$, $\eta_p^2 = .163$. Those in the high accuracy condition perceived surveillance to be more accurate ($M = 4.87$, $SD = 1.01$) than did those in the medium condition ($M = 3.89$, $SD = 1.01$; $p < .001$). Those in the medium condition also perceived surveillance as slightly more accurate than those in the low accuracy condition ($M = 3.82$, $SD = 1.31$);

however, this was not a significant difference (p = .746). As the overall effect was significant and the mean values demonstrate the predicted trend the manipulation was considered a qualified success.

Table 1. Correlations between measures

Variable	1.	2.	3.	4.
1. Recognition	-			
2. Privacy concern	-.16	-		
3. Visibility	.004	.25**	-	
4. Accuracy perceptions	.32***	.05	.23**	-
5. Feelings towards surveillance	.24**	-.49***	-.47***	-.03

Note. *p < .05, **p < .01, ***p < .001.

Hypothesis testing

Feelings towards surveillance. A one-way between-participants ANOVA did not reveal an effect of accuracy of surveillance on feelings towards surveillance, $F(2, 148) = 0.99$, $p = .375$, $\eta_p^2 = .013$. However, in light of previous work which has highlighted level of internet use as an important moderator of online behaviour, a 2-way ANOVA was performed, with internet use (continuous) as a second independent variable. The main effect of accuracy was again not significant, $F(2, 141) = 0.88$, $p = .418$, $\eta_p^2 = .012$, nor was the main effect of internet usage, $F(1, 141) = 0.05$, $p = .829$, $\eta_p^2 = .000$. However, the interaction between accuracy and internet usage was marginally significant (Figure 3), $F(2, 141) = 2.82$, $p = .063$, $\eta_p^2 = .038$.

The simple main effect of surveillance accuracy for low users (scoring 1SD below the mean) was not significant, $F(1, 141) = 1.63$, $p = .200$, $\eta_p^2 = .023$, nor was the simple main effect for high users (scoring 1SD above the mean), $F(1, 141) = 2.17$, $p = .118$, $\eta_p^2 = .030$. However, for high users, simple pairwise comparisons revealed that those in the high accuracy condition ($M = 3.08$) had significantly more negative feelings towards surveillance than those in the medium accuracy condition ($p = .039$). Furthermore, high internet users in the medium accuracy condition had more positive emotions ($M = 3.77$) than those in the low accuracy condition ($M = 3.40$), however this difference was not significant ($p = .326$). There was no significant difference in feelings towards surveillance between the high and low condition ($p = .412$). Therefore, results illustrated a non-linear trend of accuracy, whereby positive feelings towards surveillance peaked when surveillance was of medium accuracy. None of the pairwise comparisons were significant for low internet use, although a non-linear trend of the opposite from to that of high internet use was apparent.

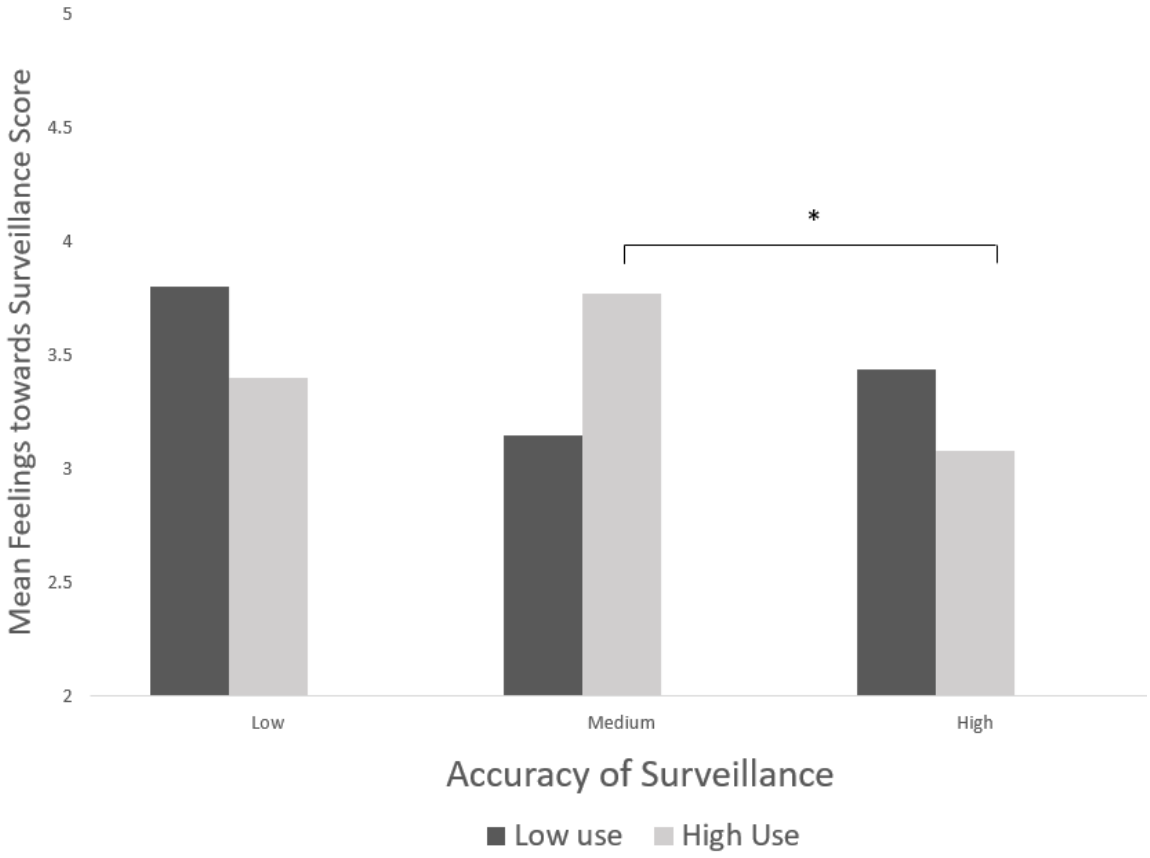


Figure 3. Feelings towards algorithmic surveillance as a function of surveillance accuracy. Low internet use is a score 1SD below the mean for internet use and high internet use is a score 1SD above the mean.

A post-hoc contrast analysis was conducted at both high and low levels of internet use, to assess whether the curvilinear trends were statistically significant (contrast weights used: -1, 2, -1). A marginally significant curvilinear trend was found at high levels of internet use: $F(1, 141) = 3.18$, $p = .077$, η_p^2 .022; however the trend was not significant at low levels: $F(1, 141) = 2.63$, $p = .107$, η_p^2 .018.

Privacy concerns. A similar 2-way ANOVA on privacy concerns did not reveal a significant simple main effect for accuracy, $F(2, 142) = 0.85$, $p = .431$, η_p^2 .012, nor internet use, $F(1, 142) = 2.45$, $p = .120$, η_p^2 .047. Only a significant

two-way interaction was found between surveillance accuracy and internet use (Figure 4), $F(2, 142) = 3.80$, $p = .025$, η_p^2 .051. The simple main effect of surveillance accuracy was significant for high internet use $F(1, 142) = 3.36$, $p = .038$, $\eta_p^2 = .045$, but was not significant for low internet use $F(1, 142) = 1.33$, $p = .268$, $\eta_p^2 = .018$. Simple pairwise comparisons revealed that for high internet use, those in the high accuracy condition ($M = 5.24$) had significantly greater concerns than in the medium accuracy condition ($M = 4.48$; $p = .011$). While not significant, mean scores reveal a trend in high users in the medium condition reporting fewer privacy concerns than those in the low accuracy condition ($M = 4.75$).

A post-hoc contrast analysis was conducted for both high and low internet use to assess the presence of a curvilinear trend (contrast weights used: -1, 2, -1). A significant trend was found for high internet use, whereby privacy concerns peaked at low and high levels of accuracy: $F(2, 142) = 3.36$, $p = .038$, $\eta_p^2 = .045$; however the trend was not significant for low internet use: $F(2, 142) = 1.33$, $p = .268$, $\eta_p^2 = .018$.

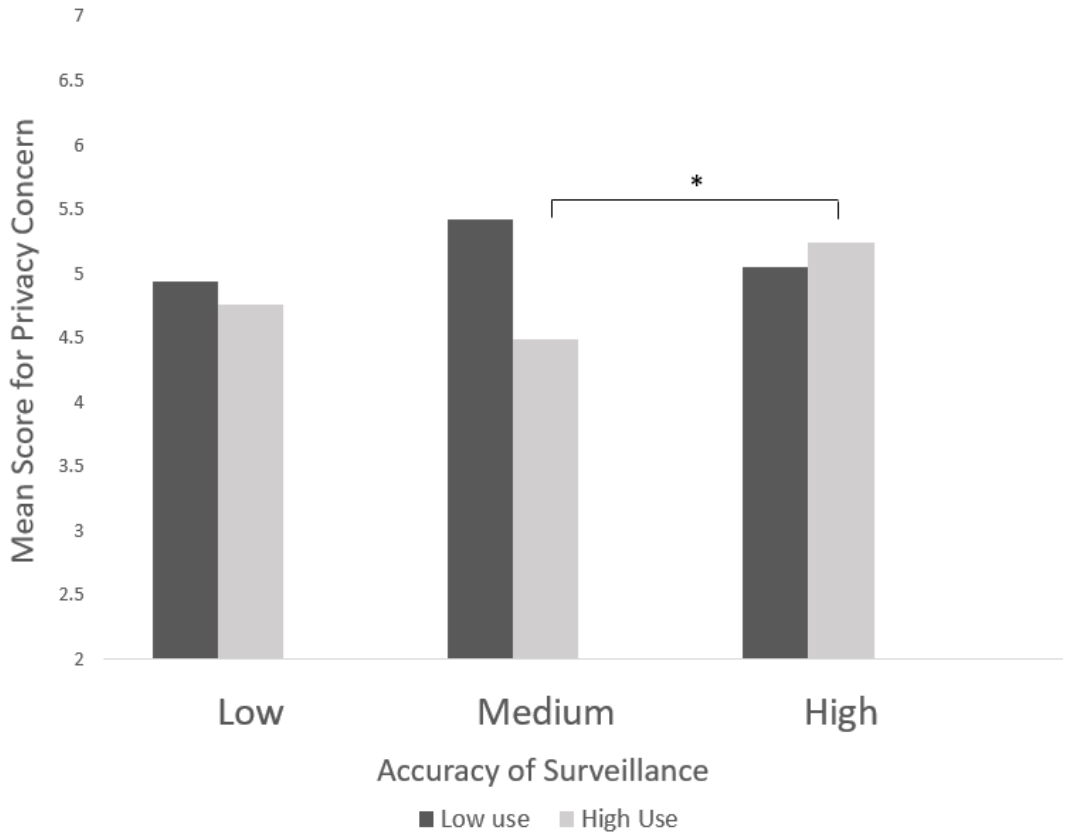


Figure 4. Privacy concern as a function of surveillance accuracy. Low internet use is a score 1SD below the mean for internet use and high internet use is a score 1SD above the mean.

Perceived visibility. A 2-way ANOVA on visibility did not reveal an interaction between surveillance accuracy and time spent online $F(2, 142) = 0.34$, $p = .709$, $\eta_p^2 = .005$. However a main effect of surveillance accuracy was found, $F(2, 142) = 3.24$, $p = .042$, $\eta_p^2 = .044$ Specifically, those in the high accuracy condition ($M = 6.65$) felt more visible than those in the low accuracy condition ($M = 6.07$; $p = .010$). All other pairwise comparisons were non-significant but followed the expected trend, whereby comparatively more accurate surveillance was associated with greater feelings of visibility.

Perceived recognition. A similar 2-way ANOVA on recognition did not reveal an interaction between surveillance accuracy and time spent online, $F(2, 140) = 0.51$, $p = .600$, $\eta_p^2 = .007$ and the main effect of surveillance accuracy did not reach significance either, $F(2, 140) = 1.58$, $p = .209$, $\eta_p^2 = .022$. However, a main effect was found for internet use, $F(1, 140) = 5.11$, $p = .025$, $\eta_p^2 = .035$. A linear regression was conducted, which illustrated that more time spent online predicted greater feelings of recognition, $b = .18$, $\beta = .19$ $SE = .08$, $p = .031$.

Do psychological outcomes predict feelings towards surveillance? A multiple regression analysis was conducted to investigate whether privacy concerns, perceived visibility, and recognition predicted feelings towards surveillance. The overall model was significant and explained 39% of the variance (R^2adj = .39, $F(3, 143) = 32.30$, $p < .001$). Results are presented in Table 1.

Each of the predictors uniquely predicted feelings towards surveillance (see Table 1). Privacy concerns negatively predicted feelings towards surveillance, in that more concerns predicted more negative feelings. As expected, recognition positively predicted feelings towards surveillance, with more perceived recognition predicting more positive feelings towards surveillance. Visibility also predicted feelings towards surveillance, but this was not in the expected direction, as greater visibility predicted more negative feelings towards surveillance.

Table 2. Multiple Regression Analysis Investigating the Relationship Between Psychological Outcomes and Feelings Towards Surveillance

IV	*b*	β	*SE*	*p*	95% CI (lower bound)	95% CI (upper bound)
Visibility	-.44	-.37	.08	< .001	-0.59	-0.28
Recognition	.23	.18	.08	.006	-.07	-0.39
Privacy concern	-.40	-.37	.07	<.001	-0.54	-0.26

Post-hoc: Moderated mediation analysis

A moderated mediation analysis was conducted using the SPSS PROCESS macro (Model 8; Hayes, 2013), which tested whether time spent online moderated the effect of surveillance accuracy on both privacy concern and feelings towards surveillance. Sequential coding was used, whereby surveillance accuracy was divided into two dummy variables: low versus medium and medium versus high. The mediator model was significant: R^2 = .08, $F(5, 141) = 2.33$, p = .046, as was the outcome model, R^2 = .27, $F(6, 140) = 8.67$, $p < .001$.

Low versus medium accuracy*. Privacy concern.* Privacy concern did not differ between those in the low and medium surveillance accuracy conditions, (b = .11, p = .629, SE = .23, 95% CI [-0.35, 0.57]). Additionally, no interaction was found between time spent online and accuracy: b = -.38, p = .133, SE = .25, 95% CI [-0.88, 0.12].

Feelings towards surveillance. There was no relationship between surveillance accuracy and feelings towards surveillance (b = -.08, p = .718, SE

= .22, 95% CI [-0.52, 0.36]). There was also no interaction between surveillance accuracy and time spent online (*b* = .32, *p* = .199, *SE* = .24, 95% CI [-0.17, 0.80]). However, privacy concern significantly predicted feelings towards surveillance; those with greater privacy concerns had less positive feelings towards surveillance: *b* = -.53, *p* < .001, *SE* = .80, 95% CI [-0.69, -0.37]. There was no indication of moderated mediation (a conditional indirect effect): Index = .20, *SE* = .14, 95% CI [-0.03, 0.53].

Medium versus high accuracy. ***Privacy concern.*** Privacy concern did not differ between those in the medium and high surveillance accuracy conditions, (*b* = .17, *p* = .434, *SE* = .22, 95% CI [-0.26, 0.60]). However, an interaction was found between accuracy and time spent online: *b* = .48, *p* = .031, *SE* = .22, 95% CI [0.04, 0.91], whereby privacy concern was greater at high levels of accuracy compared to medium surveillance accuracy for high internet use, *b* = .56, *SE* = .28, *t* = 1.98, *p* = .050, 95% CI [0.001, 1.11], but not for low internet use, *b* = -.26, *SE* = .29, *t* = -0.90, *p* = .372, 95% CI [-0.84, 0.32].

Feelings towards surveillance. There was no relationship between surveillance accuracy and feelings towards surveillance (*b* = -.12, *p* = .577, *SE* = .21, 95% CI [-0.53, 0.29]). There was also no interaction between surveillance accuracy and time spent online (*b* = -.25, *p* = .252, *SE* = .21, 95% CI [-0.67, 0.18]). There was no indication of a moderated mediation (a conditional indirect effect): Index = -.25, *SE* = .14, 95% CI [-0.57, 0.0003].

Discussion

This first study tested whether the effect of surveillance accuracy on feelings towards surveillance would be explained in part by two countervailing pathways: one negative through privacy concern, and one positive through

recognition. We also aimed to test whether visibility would have a positive association with feelings towards surveillance.

Surveillance accuracy's effect on feelings towards surveillance

There was no main effect of surveillance accuracy on feelings towards surveillance. However, as with prior internet-based research (Wilkins et al., 2017), there was some evidence of an effect when internet use was considered as a moderator. A curvilinear trend was found for high internet use; feelings towards surveillance became more positive when accuracy increased from low to medium, and became more negative when accuracy increased from medium to high. However, the only consistently significant difference was between medium and high levels of accuracy. This is supportive of previous research which has found that highly-accurate surveillance can reduce positivity towards surveillance, as the surveillance comes to be seen as creepy (Ur et al., 2012; Tene & Polonetsky, 2014).

Our findings build upon this research by presenting further possible explanations as to why highly-accurate surveillance can foster negativity. Whilst highly-accurate surveillance may offer opportunities for recognition – which in turn fosters more positive feelings towards surveillance – favourability towards surveillance is likely to be offset by increases in privacy concern. As suggested in prior literature (Tene & Polonetsky, 2014; Ur et al., 2012), we found that less accurate (but not highly inaccurate) surveillance was associated with more positive feelings towards surveillance. Specifically, in the current study we found that surveillance of medium accuracy balances the needs best for those that use the internet a lot. At medium levels of surveillance accuracy, individuals perceive the best opportunity for recognition whilst maintaining acceptable levels of privacy. In this instance, the internet may be considered one of life's

stages (Goffman, 1959), on which identity is both formed, enacted, and potentially recognised (Greenhow & Robelia, 2009). The role of these potential mediators is discussed below.

Privacy concerns

We did not find the expected positive relationship between surveillance accuracy and privacy concerns. Instead, a curvilinear trend was found for high users only. Despite this, privacy concerns only significantly differed between medium and high levels of accuracy; concerns peaked when accuracy increased from medium to high. The findings thus only partially support our initial prediction that privacy concerns increase as accuracy increases. This corroborates previous research, in that highly-accurate surveillance can elicit privacy concerns because it makes it salient that an individual is being observed and tracked (Ur et al., 2012). Therefore, while organisations have purposely implemented flawed targeted advertising to reduce concerns for customers (Duhigg, 2012), the current study provides the first empirical indication of a 'tipping point' (or at least a non-linear effect) for surveillance accuracy in terms of how positively or negatively it is perceived.

The findings also support the hypothesis that greater privacy concerns would predict more negative feelings towards surveillance. This is in line with research by Pavone and Esposti (2010), who found that individuals who felt negatively towards surveillance believed it to be an inherent invasion of privacy. Therefore, the present study supports previous findings that the degree to which we believe surveillance threatens our privacy predicts how favourably we perceive surveillance.

Visibility

As predicted, recognition functioned differently from visibility in our model: results demonstrated that recognition had a predictive role over and above mere visibility when understanding feelings towards surveillance. Whilst visibility can facilitate recognition (Brighenti, 2007) the two are conceptually distinct. Additionally, surveillance accuracy was found to affect perceived visibility, in that the more accurate the surveillance, the more visible participants felt. To our knowledge, this is the first study to demonstrate that the accuracy of surveillance (as distinct from its presence or absence per se; Marthews & Tucker, 2017; Oulasvirta et al., 2012) can affect perceived visibility online.

Whilst visibility was found to predict feelings towards surveillance, this was in the opposite direction to that hypothesised. Participants felt *less* positive towards surveillance when levels of perceived visibility were greater. This hypothesis was based on the reasoning that visibility was desirable, as it facilitates social inclusion, recognition, and empowerment (Brighenti, 2007; Skeggs, 1999). Nevertheless, the present results echo evidence that in some circumstances, greater visibility is not necessarily welcomed. For example, supra-visibility can encourage discriminatory practices, as supra-visible individuals are more likely to be caught for misdemeanours than those who are less visible (Brown, 2013). Furthermore, being visible does not guarantee individuals are visible in the way they would like to be. As argued by Brighenti (2007), ‘distortions in visibility lead to distortions in social representations’ (p. 330). For example, Muslim identity at a collective level is highly visible in the media, yet the representation of the identity is not necessarily favourable (Blackwood et al., 2013). Finally, being supra-visible encourages higher levels of impression-management strategies, which can be psychologically draining

(Steeves & Bailey, 2016). Therefore, while these findings did not support initial hypotheses, the results echo previous research investigating responses to supra-visibility.

It is also important to note that previous research finding a favourable response to visibility are those that focus on individuals typically struggling for a social presence (e.g. teenagers; boyd, 2014; Steeves & Bailey, 2016). As the majority of participants in the present study were white, British, and middle aged, visibility may have been less of a motivating factor.

Recognition

The findings did not indicate that accuracy of surveillance affected perceived recognition. This contrasts with previous social-veillance research, whereby surveillance from peers can result in identity recognition when those surveilled feel accurately perceived (Mann & Ferenbok, 2013; Kennedy, 2006). One methodological factor may help to account for the present null finding: the recognition measure followed eight other measures, meaning that the effects of the manipulation may have subsided by the time participants completed the recognition scale (no effects were evident on other variables assessed later in the questionnaire). Our subsequent studies addressed this possibility by placing the recognition measure earlier in the questionnaire.

Perhaps more importantly, the need for recognition may not have been made salient for the participants, as no specific social identity was made salient. Self-categorisation theory (SCT) suggests that an individual's context determines which identity is the most salient at any given time (Rydell, McConnell, & Beilock, 2009; Turner, Hogg, Oakes, Reicher, & Wetherell, 1987). In this study we did not employ an identity-relevant context that would have rendered a specific social identity more salient than another. As such, it was

also unlikely that identity-related concerns were salient for the participants. Without a concern for one's identity, participants are unlikely to register opportunities for recognition, as the need for recognition is not salient. Consequently, participants were unlikely to have felt more or less recognised as a result of the manipulation.

In terms of the predictive effects of recognition, the results were consistent with the hypothesis that greater levels of recognition would be associated with more positive feelings towards surveillance. This is consistent in a broad sense with SIT (Tajfel & Turner, 1979), which suggests that individuals are motivated for their social identity to be seen accurately and positively by others, and that this recognition results in positive psychological outcomes (e.g., self-esteem; Steeves & Bailey, 2016). Thus, the current study offers a counterpoint to previous literature that emphasises the negative psychological consequences of surveillance (Marthews & Tucker, 2017; Oulasvirta et al., 2012), as the present study illustrates a potential positive psychological component.

Limitations

The findings above are discussed in relation to high internet use only, as unexpectedly the same was not found for low internet use. Instead, low internet use showed the opposite trend, as feelings were least positive towards surveillance and privacy concern was greatest when accuracy was medium. However, this trend was neither significant nor consistent. It could be argued that unlike those who use the internet a lot, those who report less internet use may not consider the internet a relevant context in which to engage in identity processes. For example, Joiner and colleagues (2007) found that low internet users had less of an affinity to others online and were less likely to feel part of

an online community. Therefore, identity concerns (such as the need for recognition) may simply not have been relevant for these individuals.

Additionally, those that do not use the internet often may have less of an understanding regarding the consequences of surveillance accuracy. For example, in Ellis et al.'s (2013) research, some participants spoke about how they were aware of surveillance, but were not sure how this affected them: 'Erm so I know there are things going on in the background but how all of this information gets to be processed that I don't know' (p. 723). This would suggest that the effects of surveillance accuracy may be more inconsistent for individuals who are less proficient online, as they are uncertain as to how their information is used and processed.

As discussed, the present study did not make salient a specific social identity. As such, identity concerns – such as the need for recognition – were unlikely to be raised during the experiment. To remedy this, our subsequent studies aimed to test our hypotheses in contexts in which a social identity was explicitly salient. Additionally, as we aimed to make salient *social* identity, we amended our recognition measure to reflect this. In the subsequent chapters we measured group-based recognition, as opposed to individual/personal-based recognition.

Social identity concerns may be made salient in two ways. Firstly, they may be shaped by the perceived identity of the surveiller, as this can potentially affect the presumed motivation for surveillance. That is, reactions to surveillance are also likely to be shaped by who we assume to be surveilling us: are they ingroup or outgroup members, and how does this shape the intentions that we assume they have? For example, Klein and Azzi (2001) found that self-presentation efforts (through strategic selection of stereotypic traits) only

occurred when the audience was an outgroup, rather than an ingroup. As a result, social identity concerns (and thus recognition concerns) may be made salient when the relationship with the surveiller is known. Additionally, we may trust the surveiller differently depending on their group membership. Typically, ingroup members are trusted to a greater extent than outgroup members (Tanis & Postmes, 2005). Trust may in turn shape individuals' reactions towards surveillance. This was the focus of Chapter 3, which aimed to make recognition concerns salient using intergroup contexts.

Secondly, social identity concerns may be more acute when a stigmatised identity is salient. The need for recognition has typically been demonstrated within minority groups (Blackwood et al., 2015; Brighenti, 2007; Skeggs, 1999; Taylor, 1994). Indeed, devalued groups have been shown to strategically select positive stereotypes to achieve positive distinctiveness (Klein & Azzi, 2001). As a result, the accuracy of surveillance may be more relevant for a group whose identity is stigmatised, as self-presentational concerns are heightened. Therefore, our aims in the studies reported in Chapter 4 included recruiting participants from marginalised/chronically misrecognised groups in order to make recognition needs salient.

CHAPTER 3

A key aim of this project is to test whether the experience of algorithmic surveillance can have both negative and positive impacts. The negative pathway is associated with privacy concerns (and is more commonly associated with surveillance). However, we also posit a potentially positive pathway associated with the concept of psychological recognition. Study 1 provides some supportive evidence for the negative pathways – but more limited support for the idea of a positive pathway through recognition. In this chapter, we attempt to develop the study of surveillance and recognition in a more theoretically-informed fashion. We build on the argument that the recognition effect may have failed to materialise because no relevant social identity was made salient. Moreover, no intergroup relationship was operationalised in Study 1, and so it was unclear to whom participants may (or may not) have felt recognised. As such, this chapter describes three studies which examine the intergroup context of *group-based* recognition and the potential positive and negative pathways associated with surveillance when social identity is made salient.

Intergroup surveillance and group-based recognition

The group membership of a surveiller may influence the degree to which we experience group-based recognition from (accurate) surveillance. Specifically, an outgroup surveiller may make identity concerns salient and increase the need for group-based recognition compared to an ingroup surveiller. Indeed, SCT posits that individuals identify with multiple social groups, and the most salient identity at any given time depends on an individual's context, such as audience (Rydell et al., 2009; Turner et al., 1987).

Group membership of an audience can determine the content of the ingroup's meta-perceptions or meta-stereotypes. Meta-stereotypes are 'beliefs regarding the stereotype that outgroup members hold about his or her group' (Vorauer, Main, & O'Connell, 1998, p. 917). Typically, individuals perceive outgroups to view their group negatively or inaccurately (Finkelstein, Ryan, & King, 2013; Sigelman & Touch, 1997; Vorauer et al., 1998) – thus, meta-stereotypes are often unfavourable. Conversely, the ingroup is assumed to hold accurate (and typically positive) perceptions of the individual (Gómez, Seyle, Huici, & Swann, 2009; Klein & Azzi, 2001). As such, an outgroup audience is more likely to elicit identity-related concerns, as the audience's perceptions are assumed to contradict an individual's own self-concept. The extent and nature of the discrepancy may also constitute identity threat (Branscombe et al., 1999; Vorauer et al., 1998). Consequently, an audience may elicit identity-related concerns if they are perceived to be a relevant outgroup.

Accurate surveillance may provide an opportunity to assuage identity-related concerns and/or improve group-based recognition. Research has demonstrated that identity-related concerns often provoke strategic behaviours that mitigate concerns or address identity threat. For example, SIDE argues that an audience prompts two identity-related processes: one cognitive and the other strategic (Reicher et al., 1995; Spears & Lea, 1994). Firstly, the characteristics of one's audience can make a particular identity salient (cognitive). Secondly, an audience creates boundaries in which to express an identity (strategic). For example, depending on one's audience, an individual may choose to conceal an identity altogether (Barreto, Ellemers, & Banal, 2006; Newheiser & Barreto, 2014) or withhold only aspects of their identity whilst

exaggerating others (Barreto, Spears, Ellemers, & Shahinper, 2003; Klein & Azzi, 2001; Saroglou, Yzerbyt, & Kaschten, 2011).

Individuals typically engage in identity-management practices based on assumed audience expectations and/or to create/maintain an identity (Baumeister, 1982). Leary and Kowalski (1990) propose that impression management is comprised of two processes: impression motivation and impression construction, both of which are largely influenced by one's audience. Impression motivation is the degree to which one is motivated to shape others' perceptions. For example, one may become more motivated to engage in impression management if they believed others' perceptions of them were discrepant from the perception that they hold of themselves. The second process – impression construction – concerns the logistics of managing others' impressions. For example, the way in which an individual constructs their identity depends on what the audience is inferred to value or expect. Together this literature suggests that an individual's audience can elicit specific identity related concerns and motivations. In turn, individuals may engage in strategic behaviours to shape others' perceptions of their group. In this chapter we propose that accurate surveillance is an avenue through which groups may increase group-based recognition.

Indeed, research has demonstrated that the presence of an outgroup encourages individuals to engage in identity-related strategic behaviour. This was demonstrated by Klein and Azzi (2001), who found that individuals visible to an outgroup were more likely to endorse positive traits belonging to the meta-stereotype than negative ones. Strategic trait selection did not occur when participants were in the presence of an ingroup. The authors argued that negative meta-stereotypes are experienced as identity threat, and as such,

participants will use opportunities to manipulate outgroup's perceptions. This is further supported by evidence on helping behaviour; individuals are more likely to help an outgroup member when they believe the outgroup views the ingroup negatively (Hopkins et al., 2007). However, individuals are not more likely to help a fellow ingroup member despite group-related concerns (van Leeuwen & Täuber, 2012).

Further evidence suggests that online contexts may facilitate strategic identity performance. Online platforms often afford users more freedom to curate their identity in ways that align with their self-concept (boyd, 2014). Specifically, visibility is amplified in online spaces, which may encourage individuals to engage in identity performances and challenge misconceptions about their group (Klein et al., 2007). For example, CMC can facilitate the development of more positive attitudes towards an outgroup when participants are provided with stereotype-disconfirming information (Alvídrez, Piñeiro-Naval, Marcos-Ramos, & Rojas-Solís, 2014). Together, this suggests that an outgroup audience is more likely to provoke group-identity concerns and, if given the opportunity, ingroup members will attempt to challenge negative perceptions that may be held against them.

Interactive effects of surveiller identity and surveillance accuracy on group-based recognition. As discussed in Chapter 1, group-based recognition may only increase if surveillance is believed to be accurate (Campbell & Wright, 2008; Marwick, 2012; McDonald & Cranor, 2010; Steeves & Bailey, 2016; Tayor, 2007). Within intergroup contexts, more accurate surveillance may only be associated with greater group-based recognition when the surveiller belongs to the outgroup. As the outgroup is assumed to hold negative meta-stereotypes (Finkelstein et al., 2013; Sigelman & Tuch, 1997;

Vorauer et al., 1998), outgroup surveillance of higher accuracy may improve group-based recognition, as it may challenge these stereotypes. Outgroup surveillance of lower accuracy may be associated with perceptions of misrecognition, as negative meta-stereotypes are not challenged by accurate information. In this instance, those surveilled may perceive no recognition benefits and may instead experience identity threat in the form of misrecognition.

On the other hand, surveillance from an ingroup is unlikely to provide recognition benefits – irrespective of its accuracy – as ingroup members are not expected to endorse the content of negative meta-stereotypes and are believed to mirror one's own perception of the ingroup (Gómez et al., 2009; Klein & Azzi, 2001). Consequently, we predict that surveiller identity moderates the effect of surveillance accuracy on group-based recognition; a linear relationship between surveillance accuracy and group-based recognition is only expected for outgroup and not ingroup surveillance.

Effects of surveiller identity and surveillance accuracy on privacy concerns

There may be several possible outcomes regarding the effects of surveillance accuracy and surveiller identity on privacy concern. Firstly, surveiller identity may have independent effects on privacy concern. Based on previous literature, ingroup surveillance could either elicit greater or fewer privacy concerns. For example, O'Donnell and colleagues have found that ingroup surveillance is associated with less privacy concern (O'Donnell et al., 2010a) or *more* concern (O'Donnell et al., 2010b) in comparison to outgroup surveillance. O'Donnell et al. (2010a) argues that surveillance from an ingroup may elicit fewer privacy concerns when it is thought to increase ingroup safety.

In these cases, ingroup surveillance may be considered necessary for ingroup welfare. Alternatively, surveillance from the ingroup in contexts where it is not considered necessary (e.g., in the workplace) may be perceived negatively, as it is not considered necessary (O'Donnell et al., 2012; Subašić, Reynolds, Turner, Veenstra, & Haslam, 2011). In each of the following three studies we used one of two intergroup contexts: surveillance in University Departments (Biosciences vs Psychology) and in international relations (American vs British). Either of these contexts could arguably be interpreted as 'necessary' surveillance. Based on O'Donnell's work, we have a non-directional hypothesis whereby ingroup (vs. outgroup) surveillance may be associated with either greater *or* fewer privacy concerns.

To our knowledge, there is no current evidence on the effects of both surveiller identity *and* surveillance accuracy or any potential interactive effects. In light of this we made tentative predictions regarding potential interactive effects between surveiller identity and surveillance accuracy. Firstly, we predicted that greater surveillance accuracy may be associated with greater privacy concerns for an outgroup surveiller but not an ingroup surveiller. In this case, inaccurate surveillance may lead to more negative outcomes for a surveilled group because the motives of the outgroup are believed to be less positive (Tanis & Postmes, 2005). On the other hand, surveillance accuracy may not affect privacy concerns for the ingroup, as those surveilled may be more likely to believe the surveiller will use their data with good intentions, irrespective of its accuracy. Additionally, variations in accuracy may be considered inconsequential, as fellow ingroup members are already assumed to have an intimate knowledge of the ingroup (Klein & Azzi, 2001) and are therefore best equipped to recognise any inaccuracies.

The role of trust: A potential mediator between surveiller identity and psychological outcomes

In addition to the predicted interactive effects between surveiller identity and surveillance accuracy, we predict that surveiller identity may have indirect effects on privacy concern and group-based recognition through trust. Typically, ingroup members are trusted to a greater extent than outgroup members (Tanis & Postmes, 2005; Foddy, Platow, & Yamagishi, 2009). In turn, trust should predict the degree to which individuals experience group-based recognition and privacy concern.

Trust should predict greater group-based recognition. More trust in the surveiller should predict a greater experience of group-based recognition. Previous research has found that trust is related to shared values and respect (Brashear, Boles, Bellenger, & Brooks, 2003). As such, when a surveiller is afforded more trust, individuals may in turn believe that the surveiller will make efforts to appraise their group in ways that mirror the group's self-concept. Taken together, we predict that an ingroup surveiller will be trusted to a greater extent, which will in turn predict more group-based recognition.

Trust should predict privacy concern. Greater trust in the surveiller should also alleviate privacy concern. Healthcare research has found that patients have less privacy concern regarding their medical records when they trust their health professional (Rohm & Milne, 2004). In online contexts, individuals are more likely to share personal information on trusted platforms compared to platforms that are less trusted (Dwyer, Hiltz, & Passerini, 2007). In their study, Dwyer et al. (2007) found that Facebook users typically trusted their chosen platform to a greater extent than MySpace users; in turn, Facebook users were more likely to disclose identifying information on the platform.

Consequently, as ingroup members are typically afforded more trust, we predict an ingroup surveiller may be trusted to a greater extent and in turn raise less privacy concern.

Overview of studies

Three studies were conducted whereby the identity of the surveiller was manipulated (ingroup vs outgroup) along with surveillance accuracy (low, medium, and high). We suggested that in Study 1, no effect of surveillance accuracy on recognition was found because identity concerns (and thus recognition needs) were not made salient. Therefore, Studies 2a, 2b, and 2c[13] aimed to raise social identity concerns by making participants aware of the surveiller's social identity. Secondly, the studies tested whether the surveiller's identity moderates the relationship between surveillance accuracy and group-based recognition; an effect of surveillance accuracy on group-based recognition is only expected when the surveiller is a relevant outgroup. The first two studies recruited Psychology students and the surveiller was described as either the Psychology Department (ingroup) or the Biosciences Department (outgroup). The third study recruited British participants and described surveillance from either British intelligence (GCHQ: ingroup) or American intelligence (NSA: outgroup). In all three studies we measured group-based recognition and privacy concern to investigate the positive and negative pathways outlined in Chapter 1. We also measured surveiller trust, to examine potential indirect effects of surveiller identity on psychological outcomes through trust.

[13] In this thesis the number designated to each study pertains to the cluster of empirical studies (studies are clustered by chapter), and the letter refers to its order in that chapter.

STUDY 2A

Study 2a tested whether surveiller identity moderates the effect of surveillance accuracy on group-based recognition and privacy concern. We also predicted a main effect between surveiller identity and psychological outcomes, and that this association may be mediated by trust. We manipulated both surveillance accuracy and surveiller identity using a University weekly bulletin. Student participants were provided with a screenshot of an online weekly news bulletin, which is typically sent to students via their student email. Within this bulletin, surveillance accuracy was either described as being of low, medium, or high accuracy and the surveiller was identified as either the Biosciences Department (outgroup) or the Psychology Department (ingroup). Our key dependent variable in Study 2a was behaviour change intentions. This departs from the main dependent variable in Study 1, which in turn is our main dependent variable in the other studies included in this thesis. Our predictions relating to behaviour change intentions are outlined below.

Behaviour change intentions

Greater group-based recognition should predict lower behaviour change intentions. Impression management literature suggests that when an individual feels misrecognised, they are more likely to modify their behaviour in order to achieve recognition. For example, those who believe they are perceived as unkind are more likely to volunteer then those who believe they are already perceived as a kind person (Hopkins et al., 2007). Additionally, individuals are more likely to endorse positive stereotypes if they believe they are perceived negatively (Klein & Azzi, 2001). Therefore, we predict that when group-based recognition is low, individuals will report greater behaviour change

intentions online, as individuals will be motivated to manage others' perceptions of the group. However, greater perceived group-based recognition will be associated with less online behaviour change intentions, as recognition needs are already met.

Greater privacy concern should predict more behaviour change intentions. We predict that higher privacy concern will be associated with greater behaviour change intentions online. Chilling effects research suggests that when individuals are concerned for their privacy they make efforts to modify their behaviour or disengage from online platforms entirely. For example, Tufekci (2008) found that individuals attempted to conceal their real identity online with nicknames or aliases when privacy concerns were high. Additionally, after the Snowdon revelations in 2013, individuals were less likely to visit privacy-sensitive Wikipedia articles than before the publicity regarding government surveillance (Penney, 2016). This suggests that higher privacy concern may predict greater behaviour change intentions, as individuals may be more incentivised to modify or limit their engagement online.

Method

Participants and design

Using purposive sampling, data were collected from 184 undergraduate students at the University of Exeter who were in the first or second year of their Psychology programme. Participants were recruited online or in person. Most participants were female (83%) and were aged between 18 and 35 years (M = 19.48, SD = 1.77). A majority (82%) identified as British, 11% identified as another European nationality and 7% were of a non-European nationality.

The study had a 2 (surveiller identity: ingroup vs. outgroup) x 3 (accuracy of surveillance: low, medium, and high) factorial between-participants design. In the outgroup surveiller condition, the surveiller was identified as the Biosciences Department, and the ingroup surveiller condition the surveiller was identified as the Psychology Department. Participants were randomly assigned to one of the six conditions. A sensitivity analysis using g*power indicated that the sample of 184 is sufficient to detect an effect size using MANOVA of $f = 0.27$ ($\eta_p^2 = .07$) with 80% power for the main effects of and interaction between surveillance accuracy and surveiller identity (two predictors; six groups). When using regression (three predictors), the current study is sufficient to detect an effect size of $f = 0.21$ (partial $r = .21$) with 80% power for each of the effects of group-based recognition, privacy concern, and trust.

Measures

Unless otherwise stated, responses were scored using a 7-point scale (1 = *Strongly disagree* to 7 = *Strongly agree*). All negatively phrased items were reverse-scored.

Manipulations. Participants were shown a fabricated University online news bulletin (Appendix C). The news bulletin described a surveillance programme to begin in the next academic year, which would only affect psychology students. To manipulate surveiller identity, the bulletin explained that the surveillance programme was to be conducted by either the Biosciences (outgroup) or Psychology (ingroup) Department. To manipulate surveillance accuracy, the programme was either described as 21% accurate (low), 50% accurate (medium), or 89% accurate (high). Students were informed in the

bulletin that they would be required to consent to the programme when enrolling for the next academic year.

Dependent measures. After reading one of the six manipulation texts, participants were asked to complete an accuracy manipulation check and measures of identification as a psychology student, privacy concern, behaviour change intentions, group-based recognition, and trust. Demographic information was then requested along with a measure of time spent logged into University Wi-Fi. A measure was also included to indicate how much participants believed the authenticity of the news bulletin. All measures may be found in Appendix D.

Manipulation check. Four items measured the extent to which the students understood the accuracy manipulation, for example 'In my view, the surveillance conducted by the Psychology department is accurate in identifying students'. However, the removal of item 3 offered an alpha increase of .06 (from α = .64). Therefore item 3 was removed prior to hypothesis-testing analyses and the remaining three items were averaged to create the final scale (α = .70, *M* = 4.26; *SD* = 1.11).

Ingroup identification. The extent to which participants identified as being a psychology student was measured using four items adapted from the identity subscale of Luhtanen and Crocker's (1992) collective self-esteem scale. This included 'being a psychology student is an important reflection of who I am'. Scores on all items were averaged to produce the final scale (α = .84, *M* = 4.70; *SD* = 1.15).

Privacy concern. Levels of privacy concern in response to the surveillance programme were measured using four items, for example 'psychology students have a right to use the University Wi-Fi without being

surveilled' and 'surveillance from the (x) Department is an invasion of privacy'. Scores on all items were averaged to produce the final scale (α = .82, *M* = 5.42; *SD* = 1.15).

Behaviour change*.* Using four items, participants were asked to indicate the extent to which they believed they would change their behaviour in response to the surveillance programme. Items included 'data surveillance from the (x) Department would make me censor what I do online while using the University Wi-Fi' and 'data surveillance from the (x) Department would not affect what I did online while using the University Wi-Fi' (reverse coded). All items were averaged to produce the final scale (α = .88, *M* = 4.54; *SD* = 1.48).

Group-based recognition**.** The extent to which participants felt that their ingroup was recognised as a result of the surveillance programme was measured using six items, such as 'the surveillance programme could distinguish how psychology students are unique from students in other departments', 'by using psychology student data, the (x) Department will accurately understand what a prototypical psychology student is like', and 'by using psychology student data, the (x) Department could understand psychology students better than I could'. Item 6 ('no matter how much data the (x) Department collects, only psychology students understand what it truly means to be a psychology student') had a poor correlation with other items and improved scale reliability by .05 (from α = .77) when removed. Therefore, item 6 was removed prior to hypothesis-testing analyses and the remaining five items were averaged to form the final scale (α = .82, *M* = 3.40; *SD* = 1.07).

Trust of surveiller. Participants completed four items which measured the levels of trust participants felt towards the surveilling department, for

example ‘I trust the intentions of the (x) Department’ and ‘surveillance conducted by the (x) Department will be for psychology students’ benefit’. All items were used to form the final scale (α = .85, *M* = 4.04; *SD* = 1.20).

Demographics. Age was requested in an open-ended format and participants were asked to indicate their gender (male, female, or other). Participants were also asked to indicate their nationality as either British, other European, or Non-European.

Time spent online. Participants indicated the number of days logged on to University Wi-Fi and how many hours they logged on per session. Responses to these two measures were then multiplied to create a variable of time spent online (total number of hours per week).

Bulletin authenticity. To establish the extent participants believed the news bulletin, participants responded to two items at the end of the study investigating the bulletin’s believability, including ‘the University news bulletin was trustworthy’.

Procedure

Paper-copy survey. Participants were predominantly approached after exiting lectures on University grounds. They were informed that the researchers were conducting a study on behalf of the University to investigate student attitudes to a new surveillance programme being introduced in the next academic year. On giving their informed consent, participants were given a screenshot of a University Weekly Bulletin, ostensibly from the University website. Once participants read the bulletin they completed the survey containing the dependent variables. On completion, participants were assured that the news bulletin was not a genuine University publication and that the

University had no intentions to implement the programme described within the bulletin. Participants were then thanked and provided with a debrief form containing various online sources regarding data privacy should they be concerned.

Online survey. Participants were recruited through social media groups accessible to the researchers. A link to the survey was posted on these groups with a brief description of the study. Once the link was opened, participants were presented with a consent page. Once consent was given, participants were randomly assigned by the software to one of the six conditions. The survey following the manipulation and the final debrief form were identical to the paper-copy materials.

Results

Manipulation checks

A two-way ANOVA was conducted to test the effect of the surveillance accuracy and surveiller identity manipulation on surveillance accuracy perceptions. A significant effect of accuracy was found on perceptions of surveillance accuracy, $F(2, 178) = 9.04$, $p < .001$, $\eta_p^2 = .092$. Those in the high accuracy condition ($M = 4.66$, $SD = 1.13$) perceived surveillance as more accurate than those in the medium accuracy condition ($M = 4.25$, $SD = 1.02$; $p = .032$). Additionally, those in the medium accuracy condition perceived surveillance as more accurate than those in the low accuracy condition ($M = 3.83$, $SD = 1.03$; $p = .034$). As such, the surveillance accuracy manipulation was considered successful. No main effect was found for surveiller identity $F(1, 178) = 0.01$, $p = .943$, $\eta_p^2 < .001$ and there was no evidence of an interaction, $F(2, 178) = 0.19$, $p = .825$, $\eta_p^2 = .002$.

Main analyses

Behaviour change intentions. A two-way ANOVA was conducted to assess the effects of surveillance accuracy and surveiller identity on behaviour change intentions (Figure 5). There was no main effect of surveillance accuracy $F(2, 178) = 0.77$, $p = .465$, $\eta_p^2 = .009$. The main effect of surveiller identity approached significance, $F(1, 178) = 2.99$, $p = .090$, $\eta_p^2 = .016$. The interaction between surveillance accuracy and surveiller identity also approached significance, $F(2, 178) = 2.46$, $p = .088$, $\eta_p^2 = .027$. Behaviour change intentions were significantly higher in the outgroup surveiller condition compared to the ingroup surveiller condition at low levels of surveillance accuracy, $F(1, 178) = 5.33$, $p = .022$, $\eta_p^2 = .029$. Behaviour change intentions did not significantly differ between groups at medium ($F(1, 178) = 0.54$, $p = .463$, $\eta_p^2 = .003$) or high ($F(1, 178) = 1.77$, $p = .186$, $\eta_p^2 = .010$) levels of surveillance accuracy.

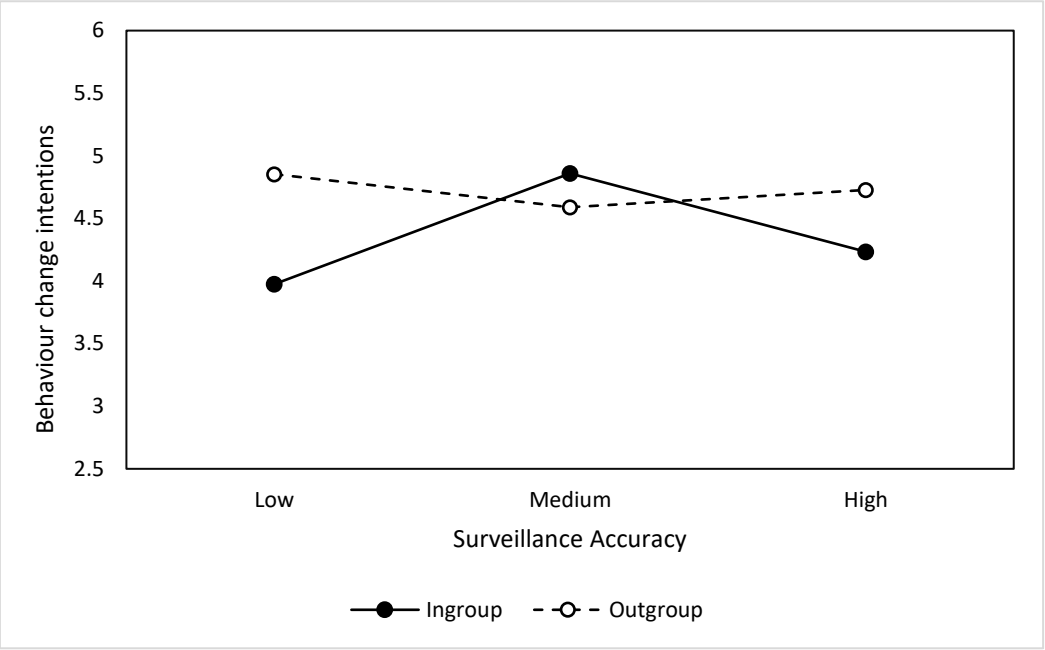


Figure 5. The conditional effect of surveillance accuracy on behaviour change intentions at the level of surveiller identity (ingroup surveillance versus outgroup surveillance).

Group-based recognition. A similar two-way ANOVA was conducted on group-based recognition. There was no main effect of surveillance accuracy $F(2, 178) = 0.71$, $p = .495$, $\eta_p^2 = .008$, nor of surveiller identity $F(1, 178) = 0.42$, $p = .519$, $\eta_p^2 = .002$. Contrary to our hypotheses, no significant interaction was found between surveillance accuracy and surveiller identity on group-based recognition, $F(2, 178) = 0.21$, $p = .813$, $\eta_p^2 = .002$.

However, whilst the accuracy manipulation did not affect group-based recognition, the measure of surveillance accuracy *perceptions* (the manipulation check) was associated with group-based recognition (see Table 3). As a post-hoc alternative test of whether the association between surveillance accuracy perceptions and group-based recognition depended on surveiller identity, we conducted a moderation analysis using PROCESS (Model 1; Hayes, 2013). No main effect was found for surveiller identity, $b = -0.05$, $se = .077$, $p = .507$, 95%

CI [-0.202, 0.100], however a main effect was found for accuracy perceptions, *b* = 0.23, *se* = .077, *p* = .003, 95% CI [0.080, 0.384] whereby perceiving surveillance as more accurate was associated with more group-based recognition. An interaction was also found between surveillance accuracy perceptions and surveiller identity on group-based recognition that was descriptively consistent with the predicted pattern (Figure 6), *b* = .15, *se* = .077, *p* = .050, 95% CI [-0.0001, 0.304]. Specifically, the relationship between surveillance accuracy perceptions was significant and positive for the outgroup, *b* = .38, *se* = .104, *p* < .001, 95% CI [0.178, 0.590], but was not significant for those under ingroup surveillance, *b* = .08, *se* = .113, *p* = .479, 95% CI [-0.143, 0.304]. Consequently, those under outgroup surveillance were more likely to report group-based recognition when surveillance was perceived as more accurate, whereas those under ingroup surveillance did not receive group-based recognition benefits when surveillance was perceived as more accurate.

Table 3. Correlations between measures

Variable	1.	2.	3.	4.	5.	6.
1. Recognition	-					
2. Privacy concern	-.30***	-				
3. Trust	.28***	-.50***	-			
4. Identification	-.01	.09	.01	-		
5. Accuracy perceptions	.23**	-.02	.11	.05	-	
6. Behaviour change	-.11	.50***	-.41***	.07	-.02	-

Note. *p < .05, **p < .01, ***p < .001.

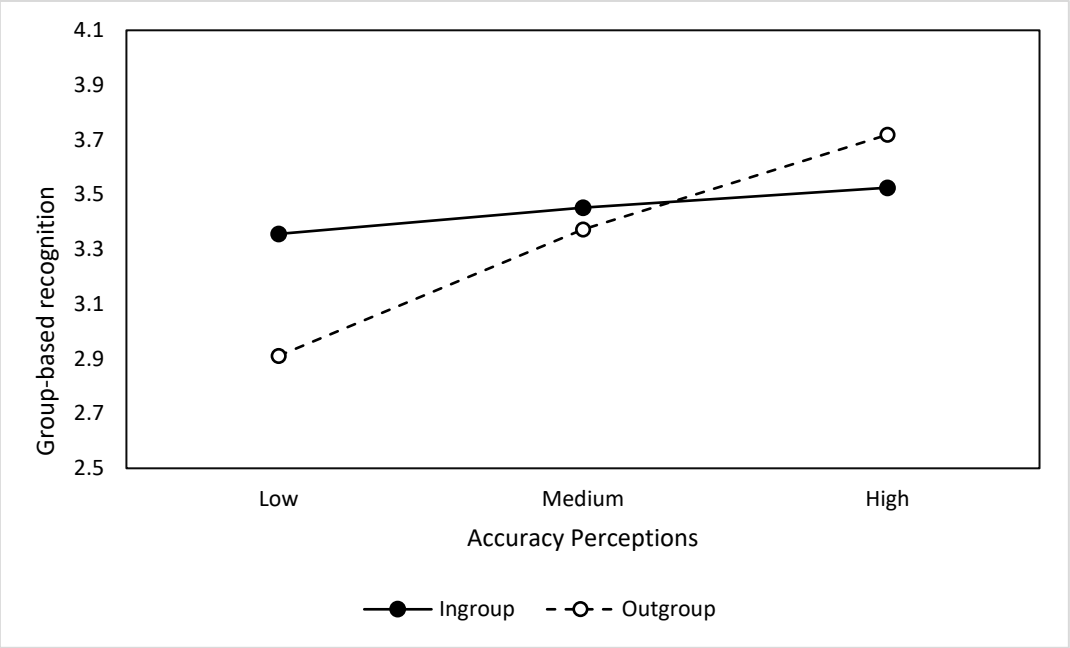


Figure 6. The conditional effect of surveillance accuracy perceptions on group-based recognition at the level of surveiller identity (ingroup surveillance versus outgroup surveillance). Low and high accuracy are valued at 1SD below and above the mean respectively. Medium is valued at the mean.

Privacy concern. A 3(surveillance accuracy: low, medium, high) X 2 (surveiller identity: ingroup, outgroup) ANOVA was conducted on privacy concerns. There was no main effect of accuracy $F(2, 177) = 0.15$, $p = .864$, $\eta_p^2 = .002$. A significant main effect was found of group $F(1, 177) = 5.59$, $p = .019$, $\eta_p^2 = .031$, with those in the outgroup condition reporting more privacy concerns ($M = 5.63$) than those in the ingroup condition ($M = 5.23$). No interaction was found between surveillance accuracy and surveiller identity on privacy concerns, $F(2, 177) = 2.30$, $p = .103$, $\eta_p^2 = .025$. A post-hoc moderation analysis was conducted in PROCESS (Model 1; Hayes, 2013) to test for an interaction between surveillance accuracy perception (i.e., the manipulation measure) and

surveiller identity on privacy concern. No main effect was found for surveillance accuracy perceptions (*b* = -.03, *se* = .085, *p* = .751, 95% CI [-0.194, 0.140]) but a main effect was found for surveiller identity (*b* = .20, *se* = .085, *p* = .020, 95% CI [0.032, 0.366]) whereby those under outgroup surveillance reported more privacy concern than those under ingroup surveillance. There was also no evidence for an interaction between surveillance accuracy perceptions and surveiller identity on privacy concern (*b* = .03, *se* = .085, *p* = .715, 95% CI [-0.136, 0.199]).

Trust. A 3(surveillance accuracy: low, medium, high) X 2 (surveiller identity: ingroup, outgroup) ANOVA was conducted on trust. There was no main effect of accuracy $F(2, 178) = 1.57$, $p = .211$, $\eta_p^2 = .017$. A significant main effect was found of group $F(1, 178) = 21.65$, $p < .001$, $\eta_p^2 = .108$, with those in the outgroup condition reporting less trust ($M = 3.64$, $SD = 1.10$) than those in the ingroup condition ($M = 4.42$, $SD = 1.18$). No interaction was found between surveillance accuracy and surveiller identity on trust, $F(2, 177) = 0.49$, $p = .613$, $\eta_p^2 = .005$. A post-hoc moderation analysis using was conducted in PROCESS (Model 1; Hayes, 2013) to test for an interaction between surveillance accuracy perception and surveiller identity on trust. No main effect was found for surveillance accuracy perceptions (*b* = .14, *se* = .085, *p* = .102, 95% CI [-0.028, 0.306]) but a main effect was found for surveiller identity (*b* = -.39, *se* = .084, *p* < .001, 95% CI [-0.557, -0.225]). There was no evidence of an interaction (*b* = -.004, *se* = .085, *p* = .964, 95% CI [-0.171, 0.163]).

The mediating role of trust. The main effect of surveiller identity on trust is consistent with previous research showing that in general, ingroup members are trusted to a greater extent than outgroup members, and individuals feel and behave more positively towards ingroup members (Brewer

& Campbell, 1976; Brewer, 1999; Foddy et al., 2009; Lonsdale & North, 2009; Tajfel, Billig, Bundy, & Flament, 1971). We predicted in turn that the effect of surveiller identity on group-based recognition and privacy concerns may be mediated by trust in the surveiller.

We conducted a mediation analysis using PROCESS (Model 4; Hayes, 2013) to test the indirect effect of surveiller identity on privacy concern via trust (Figure 7). Results revealed a significant indirect effect of surveiller identity on privacy concern through trust, *b* = .32, *se* = .076, 95% CI [0.179, 0.477]. There was no evidence that surveiller identity (ingroup vs outgroup) affected privacy concerns independently of trust (*b* = .03, *se* = .158, *p* = .859, 95% CI [-0.283, 0.339]). As such, those in the outgroup condition reported less trust in the surveiller (*b* = -.79, *se* = .169, *p* < .001, 95% CI [-1.1222, -0.454]), which in turn predicted greater levels of privacy concern (*b* = -.47, *se* = .067, *p* < .001, 95% CI [-0.598, 0.340]).

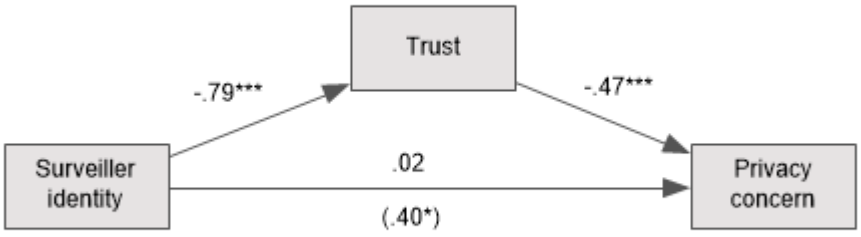


Figure 7. Path diagram illustrating the effect of surveiller identity on privacy concern through trust.

A similar analysis was conducted for group-based recognition as the dependent variable (see Figure 8). A significant indirect effect of surveiller identity was found on group- based recognition through trust, *b* = -.19, *se* =

.067, 95% CI [-0.337, -0.076]. As with privacy concerns, there was no evidence that surveiller identity (ingroup vs outgroup) affected group-based recognition independently of trust, *b* = .12, *se* = .161, *p* = .515, 95% CI [-0.213, 0.423]). Therefore, those in the outgroup condition were less likely to trust the surveiller (*b* = -.78, *se* = .168, *p* < .001, 95% CI [-1.113, -0.449]), and in turn, reported less group-based recognition (*b* = .26, *se* = .067, *p* < .001, 95% CI [0.131, 0.395]).

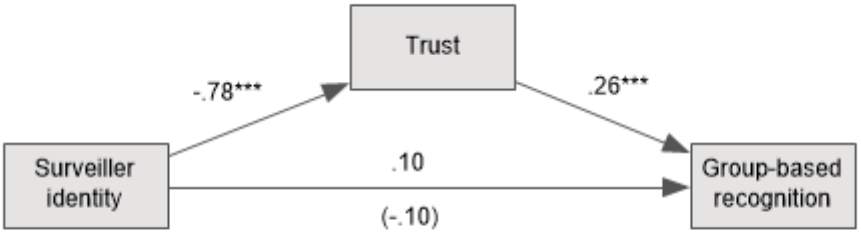


Figure 8. Path diagram illustrating the effect of surveiller identity on group-based recognition through inferred trust.

The effects of recognition, privacy concern, and trust on behaviour change intentions online

A multiple regression analysis was then conducted to investigate whether group-based recognition, privacy concerns, and trust predicted behaviour change intentions online. The overall model was significant and explained 29% of the variance (R^2 adj = .28, $F(3, 179) = 24.61$, $p < .001$). As can be seen from Table 4, greater privacy concerns and less trust were associated with stronger intentions to change online behaviour. However, contrary to predictions, recognition did not uniquely predict behaviour change intentions online.

Table 4. Multiple regression analysis investigating the relationship between psychological outcomes and behaviour change intentions online

IV	*b*	β	*t*	*p*
Recognition	.10	.07	1.06	.290
Privacy concern	.53	.41	5.58	< .001
Trust	-.28	-.23	-3.09	.002

Discussion

Study 2a aimed tested whether the effect of surveillance accuracy on online behaviour change intentions would be explained in part by two pathways: a positive pathway through group-based recognition and a negative pathway through privacy concern. We also anticipated that the positive pathway and potentially the negative pathway may be moderated by surveiller social identity. For the positive pathway, we suggested that greater surveillance accuracy would increase feelings of group-based recognition, and that this would be particularly so when the surveiller was part of the outgroup. In turn, we expected that greater group-based recognition would predict lower behaviour change intentions. We did not predict an association between surveillance accuracy and group-based recognition when surveillance was conducted by the ingroup, as recognition is already implied by shared group membership.

For the negative pathway, we proposed several possible outcomes. We predicted that surveiller identity may independently affect privacy concerns in either of two ways: ingroup surveillance may elicit more privacy concern (O'Donnell et al., 2010b), or less privacy concern (O'Donnell et al., 2010a).

Additionally, we predicted that there may be an interaction between surveiller identity and surveillance accuracy: greater surveillance accuracy may be associated with increased privacy concern only when surveillance was conducted by the outgroup, as the outgroup is assumed to have negative intentions towards the ingroup. For the ingroup, surveillance accuracy may not affect privacy concerns, as the ingroup is assumed to use group's data within its best interest irrespective of its accuracy. Additionally, variations in accuracy may be considered inconsequential, as fellow ingroup members are assumed to have first-hand knowledge of whether data accurately (or inaccurately) represents the group. In turn, greater privacy concern was predicted to increase behaviour change intentions.

Additionally, we also predicted that trust may operate as a mediator in both the positive and negative pathways. Specifically, we predicted that an ingroup surveiller would be trusted to a greater extent than an outgroup surveiller. In turn, we predicted that greater trust would predict more group-based recognition and less privacy concern.

A positive pathway through group-based recognition

Perceiving surveillance from an *outgroup* as more accurate is associated with greater group-based recognition. The surveillance accuracy manipulation did not affect group-based recognition; however, surveillance accuracy *perceptions* were associated with group-based recognition. Perceiving surveillance as more accurate was associated with more group-based recognition. This was in turn qualified by an interaction between surveillance accuracy perceptions and surveiller identity on group-based recognition. For those under outgroup surveillance, perceptions of greater surveillance accuracy were associated with more group-based recognition. On the other hand, no

association between surveillance accuracy perceptions and recognition was found for those under ingroup surveillance. This supports the premise that those under ingroup surveillance do not receive any group-based recognition benefits, as recognition is already implied through shared group identity, and suggests that surveillance from the ingroup is less likely to raise identity-related concerns compared to outgroup surveillance.

This is consistent with previous research, which demonstrate that individuals are less likely to engage in identity management strategies when in the presence of an ingroup audience compared to an outgroup audience (Klein & Azzi, 2001). Here, it could be argued that an outgroup surveiller is believed to subscribe to misconceptions about the group (Finkelstein et al., 2013; Sigelman & Tuch, 1997; Vorauer et al., 1998). Therefore, participants may believe that surveillance of greater accuracy allows the outgroup to access information that may disconfirm inaccurate or negative perceptions of the ingroup. Consequently, whilst an outgroup audience/surveiller may pose a threat to identity (as it may make meta-stereotypes salient), *accurate* surveillance from an outgroup also presents the opportunity to challenge misconceptions and foster group-based recognition.

Trust. Furthermore, the present study illustrates that an ingroup surveiller may typically be trusted to a greater extent, and that this in turn predicts more group-based recognition. Previous research has found that those under ingroup surveillance may demonstrate behavioural backlash against surveillers (e.g. less helping behaviour than when under low levels of surveillance; O'Donnell et al., 2012). However, the present study demonstrates that in some circumstances ingroup surveillers are afforded more trust, which is associated with *positive* outcomes in the form of group-based recognition.

Indeed, this is consistent with previous research that finds the ingroup is trusted to a greater extent (Tanis & Postmes, 2005; Foddy et al., 2009) and that individuals are better able to achieve recognition and affirmation through those they trust (de Laat, 2008).

No unique association between group-based recognition and behaviour change intentions. Contrary to expectations, less group-based recognition did not predict greater behaviour change intentions online. Previous research suggests that when individuals feel misrecognised, they are more likely to change their behaviour or withdraw entirely from surveilled spaces to manage others' perceptions of them (Klein & Azzi, 2001; Hopkins et al., 2007; Leary & Kowalski, 1990). Our findings did not echo this.

It could be argued that as the study concerned surveillance surrounding university Wi-Fi and university platforms, this surveillance is unavoidable. Students require Wi-Fi whilst on campus and many courses require engagement with university online platforms. As such, participants may have felt that they were not able to change or modify their online behaviour whilst at University, since online engagement is necessary for their studies. Indeed, research finds that those wishing to change their online behaviour are often restricted by social pressures (Welinder, 2012) or do not feel technologically literate enough to change their behaviour effectively (Tene & Polonetsky, 2014). This may be especially true when attempting to engage in identity management through surveillance. Individuals are often unaware of what aspects of their online behaviour are being surveilled and how this may be represented in a data format (Ellis et al., 2013). As such, participants may have felt unable to effectively change their behaviour online to manage perceptions.

A negative pathway through privacy concern

Surveiller identity (but not surveillance accuracy) is associated with privacy concern. The main effect of surveillance accuracy on privacy concerns was not significant, nor was the interaction between accuracy and surveiller identity. There was also no association between surveillance accuracy *perceptions* and privacy concern. However, a main effect of surveiller identity was found, in that surveillance conducted by the outgroup was associated with more privacy concern than surveillance conducted by the ingroup. This echoes research by O'Donnell et al. (2010a), who found that surveillance from fellow sub-group members was seen as less concerning than surveillance from a superordinate group.

Trust. Our study also extends O'Donnell et al.'s (2010a) findings by demonstrating that fewer privacy concerns from ingroup surveillance may be in part explained by greater trust for ingroup surveillers. Mediation analyses revealed that participants trusted an ingroup surveiller to a greater extent than an outgroup surveiller. In turn, greater trust predicted less privacy concern. This supports previous literature, which found that outgroup members are typically trusted less (Brewer & Campbell, 1976; Brewer, 1999; Foddy et al., 2009). The current study illustrates that intragroup trust also extends to potentially invasive behaviours, such as intragroup surveillance.

Greater privacy concern is associated with behaviour change intentions online. As expected, greater privacy concern was associated with greater behaviour change intentions online. This is consistent with research on 'chilling effects', which finds that those who are concerned for their privacy online, or are aware of aggressive surveillance practices online, are more likely to moderate their behaviour or withdraw from online platforms altogether

(Dawson et al., 2005; Marthews & Tucker, 2017; Oulasvirta et al., 2012). Whilst the current study did not explore the nature of behaviour change intentions, previous research illustrates that some individuals continue online engagement, yet use anonymising techniques, such as changing profile nicknames (Tufekci, 2008), whilst others have found individuals withdraw entirely from surveilled platforms (Starr, Fernandez, Amster, Wood, & Caro, 2008). Further research is required to explore the reasons for variation in behaviour change online when individuals are concerned for their privacy.

STUDY 2B

Study 2a suggests that surveillance can produce positive psychological outcomes in the form of group-based recognition when surveillance is *perceived* as having greater accuracy (however, the surveillance accuracy manipulation was not associated with group-based recognition). Additionally, the study provides preliminary evidence that the identity of the surveiller may moderate this effect, although the effect was weak and was only just within the conventional boundaries of statistical significance. As a result, Study 2b aims to replicate these findings and address potential limitations.

Firstly, in Study 2a the manipulation of surveillance accuracy did not affect privacy concern nor recognition. Instead, as with Study 1, only participants' *perceptions* of surveillance accuracy predicted feelings of group-based recognition. One possible reason for this is that the manipulation of surveillance accuracy may not have been strong enough. For instance, the accuracy manipulation within the online news bulletins was only present in one of the four paragraphs participants were asked to read. Consequently, whilst the manipulation check indicated a successful if modest manipulation, it may not

have been strong enough to affect participants' responses in the later measures. As such, Study 2b aimed to strengthen the accuracy manipulation by making information about accuracy more prominent in three of the four paragraphs.

Secondly, Study 2a differed from Study 1 in that feelings towards surveillance were not measured. Instead, Study 2a explored the effects of surveillance accuracy (and group-based recognition and privacy concern) on behaviour change intentions online. In Study 2b we returned our focus to the impact of group-based recognition and privacy concern on feelings towards surveillance.

Thirdly, we aimed to replicate the mediating effect of trust found in Study 2a. Here, we found that an ingroup surveiller was perceived as more trustworthy than an outgroup surveiller. In turn, greater trust predicted more group-based recognition and less privacy concern. Thus, ingroup surveillance was associated with more positive and less negative outcomes (through trust). As discussed above, our findings echo those of O'Donnell et al. (2010a), as they found surveillance from those participants closely identified with was associated with less privacy concern.

Alternatively, previous literature has also found that ingroup surveillance can *undermine* shared group membership (O'Donnell et al., 2010b), and can produce negative outcomes (less intragroup helping; O'Donnell et al., 2012). Consequently, we aim to replicate the findings from Study 2a to further clarify the circumstances under which ingroup surveillance can contribute to more positive or negative outcomes.

As such, in Study 2b we predicted an interaction between surveillance accuracy and surveiller identity on group-based recognition, whereby increases

in recognition from accurate surveillance are only evident under outgroup surveillance. We also predicted a main effect of surveiller identity, in that ingroup surveillance will be associated with more group-based recognition, as the surveiller is trusted to a greater extent.

As Study 2a did not find an interaction between surveillance accuracy and surveiller identity on privacy concern, we predicted that accuracy and surveiller identity will have independent effects. As demonstrated in Study 1, we expected surveillance of greater accuracy to be associated with more privacy concern. Additionally, we expected outgroup surveillance to be associated with more privacy concern than ingroup surveillance, and that this relationship will be mediated by trust.

As outlined in Chapter 1 and demonstrated in Study 1, we predicted that more group-based recognition will predict more positive feelings towards surveillance, and more privacy concern will predict less positive feelings towards surveillance.

In sum, Study 2b aimed to address two main limitations of Study 2a. We aimed to include more accuracy manipulation content in the news bulletin to strengthen the surveillance accuracy manipulation. Additionally, we included feelings towards surveillance as the primary dependent variable to remain consistent with the other studies of the project. Study 2b also aimed to replicate the exploratory findings suggesting that trust might mediate the relationship between surveiller identity and psychological outcomes.

Method

Participants and design

Participants were recruited through the University of Exeter research portal, SONA, which is used by undergraduate students to sign up for course credit. A total of 217 submissions were recorded; however, 17 participants were not included in the analyses as they had not completed any of the dependent measures. This left 200 participants. A majority of 83% were women (17% men, 1% non-binary) and 75% identified as being White (3% Mixed, 21% Asian, 1% Arab, 1% Other). Participants' mean age was 18.84 years (*SD* = 0.86). A sensitivity analysis using g*power indicated that the sample is sufficient to detect an effect size using MANOVA of $f = 0.22$ ($\eta_p^2 = .05$) with 80% power for the main effects of and interaction between surveillance accuracy and surveiller identity (two predictors; six groups). When using regression (five predictors), the current study is sufficient to detect an effect size of $f = 0.20$ (partial $r = .20$) with 80% power for each of the effects of group-based recognition (distinctiveness, understanding, positivity), privacy concern, and trust.

The study had a similar 3 (accuracy: low, medium, high) x 2 (group: ingroup, outgroup) between-participants design to Study 2a, and participants were assigned randomly to one of the six conditions. Dependent measures included feelings towards surveillance (positive and negative) with perceived group-based recognition (distinctiveness, positivity, and understanding), trust, and privacy concern as potential mediators.[14]

[14] Additional measures were also taken but not included in the analyses. These included measures of behaviour change intentions, visibility, and group identification. These were not included in the analyses, as they were not directly relevant to the rationale of the study. All measures may be found in Appendix F.

Materials

Unless otherwise stated, responses were collected using a 7-point Likert scale (1 = *Strongly disagree* to 7 = *Strongly agree*). Negatively-phrased items were reverse coded.

Identity salience. Based on the method used by Haslam, Oakes, Reynolds, and Turner (1999), participants were asked to write three things that they felt made those in Psychology different from those belonging to other disciplines. This was included to ensure that the Psychology identity was salient at the time of completing the survey.

Identification. Four items were adapted from the Doosje, Ellemers, and Spears' (1995) identification scale to measure ingroup (Psychology) identification. Items included 'I identify with others in Psychology' and 'I am glad to be part of Psychology'. All items were used for the final identification scale (α = .83, *M* = 5.44; *SD* = 0.84).

Manipulation. Participants were shown an ostensibly genuine University online news bulletin (Appendix E). The news bulletin described a new surveillance programme to begin in the next academic year, which would only affect Psychology students. The bulletin explained that the surveillance programme would be conducted by either the Biosciences or Psychology Department. To manipulate surveillance accuracy, the programme was described as either 21% accurate, 50% accurate, or 89% accurate. Students were informed in the bulletin that they would be required to consent to the programme when enrolling for the next academic year.

Dependent measures. ***Accuracy manipulation check.*** Four items were included to assess the effectiveness of the accuracy manipulation (e.g. 'In

my view, algorithmic surveillance conducted by the (x) Department is accurate at identifying people').[15] The four items were averaged to create the final scale (α = .79, *M* = 3.55; *SD* = 0.95).

***Perceived recognition*.** Recognition was divided into three dimensions: positivity, distinctiveness, and understanding. In Chapter 1 we outlined the potential dimensions of (group-based) recognition. As such, from Study 2b onwards we aimed to take a more nuanced approach that would enable us to explore which elements of group-based recognition were contributing to our predicted model and which dimensions may predict feelings towards surveillance. Confirmatory Factor Analysis supported our three-factor approach. These results may be found in Appendix G.

Positivity. Four items measured how positively participants felt Psychology students were perceived by others (e.g., 'We will be valued positively through the surveillance programme'). On analysis, item 2 ('Algorithmic surveillance conducted by the (x) Department would not portray us positively') did not correlate with the other three items and improved the scale's reliability by .06 (from α = .66) if removed. Therefore, item 2 was deleted and the remaining three items were averaged to create the final scale (α = .72, *M* = 4.00; *SD* = 0.91).

Distinctiveness. Four items measured the extent to which participants felt surveillance recognised those in Psychology as belonging to a distinct discipline. Items included 'Algorithmic surveillance will enable the (x) Department to recognise that we are a unique discipline'. On analysis, item 4 ('Algorithmic surveillance conducted by the (x) Department would imply that we

[15] These items were similar to those in Study 2a, but items referred to 'people' rather than 'students'.

are indistinguishable from other academic communities') did not correlate with the other three items and improved the scale's reliability by .014 if deleted. Therefore, item 4 was deleted and the remaining three items were averaged to create the final scale (α = .80, *M* = 3.70; *SD* = 1.07).

*Understanding**.*** Four items were included to measure the extent to which participants felt surveillance understood ingroup members, such as 'Algorithmic surveillance will help the (x) Department understand our values'. All four items were used to create the final scale (α = .73, *M* = 3.69; *SD* = 0.98).

***Feelings towards surveillance*.** Feelings towards surveillance were measured with two scales: positive emotion and negative emotion. Participants were asked, 'Algorithmic surveillance makes me feel…' and were then presented with 14 emotion items (seven items per scale).

Positive feelings. All seven items, such as 'happy' and 'pleased' were averaged to form the positive feelings scale (α = .93, *M* = 3.26; *SD* = 0.97).

Negative feelings. All seven items, such as 'angry' and 'anxious' were averaged to create the negative feelings scale (α = .88, *M* = 4.19; *SD* = 1.02).

Trust. Four items measured the extent to which participants trusted the department conducting the surveillance, such as 'I trust the (x) Department to gather our online data'. All items were averaged to form the final scale (α = .78, *M* = 3.96; *SD* = 1.11).

Privacy concern. Four items measured the extent to which participants felt surveillance compromised their privacy. Items included 'surveillance online is an invasion of privacy' and 'people have a right to use the internet without being surveilled'. All items were used to create the final scale (α = .60, *M* = 5.07; *SD* = 0.99).

Demographics. Participants were asked to provide their age, gender, and ethnicity. They were also asked how long they spent online, whether they belonged to closed/private groups online, and how aware they were of surveillance online (1 = *Not at all aware* to 10 = *Very aware*).

Procedure

Participants were recruited through SONA, the University's research participation system. Participants were presented with a brief description of the study before continuing to the consent form. After giving their informed consent, participants completed the pre-manipulation measures before being randomly allocated to one of the six conditions. They were then asked to read the news bulletin corresponding to their condition before completing the dependent measures. On completion or withdrawal, participants were thanked, fully debriefed, and provided with online sources pertaining to internet privacy online should they feel concerned. Participants were compensated with course credit.

Results

Missing data treatment

Analysis of missing data revealed that only 0.04% of values were missing across all measures.[16] Missing values were imputed using the expectation-maximisation (EM) method in SPSS (Graham, 2009) and estimated values fell within the scale range.

[16] Missing data analysis and treatment was used in Study 2b and onwards, as Confirmatory Factor Analysis (CFA) was used in these studies to test our predicted conceptualisation of (group-based) recognition (this was not done in Study 1 or 2a). As CFA requires complete data, missing data analysis and treatment was employed.

Manipulation checks

A two-way ANOVA was conducted to test the effect of the surveillance accuracy and surveiller identity manipulations on surveillance accuracy perceptions. A significant effect of surveillance accuracy was found on perceptions of surveillance accuracy, $F(2, 194) = 5.00$, $p = .008$, $\eta_p^2 = .049$. Those in the high accuracy condition ($M = 3.84$, $SD = 0.95$) perceived surveillance as more accurate than those in the medium accuracy condition ($M = 3.39$, $SD = 0.85$; $p = .005$). However, those in the medium accuracy condition did not significantly differ in perceived surveillance accuracy compared to those in the low accuracy condition ($M = 3.41$, $SD = 0.78$; $p = .863$). Those in the high accuracy condition reported significantly higher accuracy perceptions than those in the low accuracy condition ($p = .009$). Therefore, despite there being no significant difference between the low and medium accuracy conditions, as accuracy perceptions significantly differed between low and high and medium and high conditions, the manipulation was considered a partial success. No evidence was found for a main effect of surveiller identity $F(1, 194) = 0.43$, $p = .511$, $\eta_p^2 = .002$, nor an interaction $F(2, 194) = 0.71$, $p = .492$, $\eta_p^2 = .007$. Correlations between all dependent measures may be found in Table 5.

Table 5. Summary of Pearson correlations between variables in the predicted model

Measure	1.	2.	3.	4.	5.	6.	7.
1. Accuracy perceptions	-						
2. Positivity	.40***	-					
3. Understanding	.39***	.45***	-				
4. Distinctiveness	.44***	.54***	.54***	-			
5. Privacy Concern	-.54*	-.19**	-.28***	-.25***	-		
6. Trust	.32***	.45***	.50***	.41***	-.46***	-	
7. Positive feelings	.37***	.56***	.44***	.48***	-.40***	.58***	-
8. Negative feelings	-.21**	-.33***	-.38***	-.31***	.37***	-.67***	-.56***

Note: * $p < .05$, ** $p < .01$, *** $p < .001$.

Hypothesis testing

Feelings towards surveillance. A multivariate analysis of variance (MANOVA) was conducted with surveillance accuracy and surveiller identity as fixed factors. Positive emotion and negative emotion were entered as dependent variables. The multivariate main effect of surveiller identity was not significant, Wilks' Lambda = .99, $F = 1.29$, $p = .277$, $\eta_p^2 = .013$, nor was the multivariate main effect of surveillance accuracy, Wilks' Lambda = .99, $F = 0.27$, $p = .895$, $\eta_p^2 < .001$. There was also no indication of a multivariate interaction, Wilks' Lambda = .97, $F = 1.48$, $p = .208$, $\eta_p^2 = .015$.

Positive feelings. No main effects were found for surveiller identity, $F(1, 194) = 0.03$, $p = .874$, $\eta_p^2 < .001$, nor surveillance accuracy, $F(2, 194) = 0.49$, p

= .614, η_p^2 = .005 on positive feelings towards surveillance. Additionally, no interaction was found between surveillance accuracy and surveiller identity on positive feelings towards surveillance, $F(2, 194) = 0.89$, $p = .415$, $\eta_p^2 = .009$.

Negative feelings. No main effect was found for surveiller identity on negative feelings towards surveillance, $F(1, 194) = 1.51$, $p = .220$, $\eta_p^2 = .008$, nor surveillance accuracy, $F(2, 194) = 0.08$, $p = .924$, $\eta_p^2 = .001$. No interaction was found between surveillance accuracy and surveiller identity on negative feelings towards surveillance, $F(2, 194) = 0.89$, $p = .415$, $\eta_p^2 = .009$.

Positive psychological outcomes: group-based recognition. A second MANOVA was conducted with surveillance accuracy and surveiller identity as fixed factors. Distinctiveness, positivity, and understanding were entered as dependent variables. The multivariate main effect of surveiller identity was not significant, Wilks' Lambda = .98, $F = 1.44$, $p = .233$, $\eta_p^2 = .022$. No significant multivariate main effect was found for surveillance accuracy, Wilks' Lambda = .97, $F = 0.96$, $p = .451$, $\eta_p^2 = .015$. There was no indication of a multivariate interaction between surveillance accuracy and surveiller identity, Wilks' Lambda = .97, $F = 1.14$, $p = .339$, $\eta_p^2 = .017$.

Distinctiveness. A marginally significant main effect of surveiller identity was found on distinctiveness ($F(1, 194) = 3.34$, $p = .069$, $\eta_p^2 = .017$) with those in the ingroup condition, ($M = 3.56$, $SD = 1.14$) reporting marginally less perceived distinctiveness than those in the outgroup condition, ($M = 3.84$, $SD = 0.98$). There was no main effect of surveillance accuracy on perceived distinctiveness, $F(2, 194) = 1.71$, $p = .184$, $\eta_p^2 = .017$, and no interaction was found between surveiller identity and surveillance accuracy, $F(2, 194) = 1.33$, $p = .266$, $\eta_p^2 = .014$.

Understanding. No main effect was found of surveiller identity, $F(1, 194) = 0.03$, $p = .871$, $\eta_p^2 < .001$, or of surveillance accuracy, $F(2, 194) = 1.29$, $p = .278$, $\eta_p^2 = .013$. No interaction was found between surveillance accuracy and surveiller identity on felt understanding, $F(2, 194) = 0.20$, $p = .821$, $\eta_p^2 = .002$.

Positivity. No main effect was found of surveiller identity, $F(1, 194) = 0.03$, $p = .871$, $\eta_p^2 < .001$, or of surveillance accuracy, $F(2, 194) = 1.29$, $p = .278$, $\eta_p^2 = .013$. No interaction was found between surveillance accuracy and surveiller identity on perceived positivity, $F(2, 194) = 1.81$, $p = .167$, $\eta_p^2 = .018$.

Privacy concern and trust. A third MANOVA was conducted with surveiller identity and surveillance accuracy as fixed factors and privacy concern and trust as dependent variables. The multivariate main effect of surveiller identity was significant, Wilks' Lambda = .95, $F = 5.31$, $p = .006$, $\eta_p^2 = .052$. No significant multivariate main effect was found for surveillance accuracy, Wilks' Lambda = .99, $F = 0.44$, $p = .778$, $\eta_p^2 = .005$. There was no significant multivariate interaction between surveillance accuracy and surveiller identity, Wilks' Lambda = .98, $F = 0.85$, $p = .493$, $\eta_p^2 = .009$.

Privacy concern. No main effect was found of surveiller identity, $F(1, 194) = 1.17$, $p = .281$, $\eta_p^2 = .006$, or of surveillance accuracy, $F(2, 194) = 0.73$, $p = .484$, $\eta_p^2 = .007$. No interaction was found between surveillance accuracy and surveiller identity on privacy concern, $F(2, 194) = 1.57$, $p = .212$, $\eta_p^2 = .016$.

***Trust*.** A main effect of surveiller identity was found on trust towards the surveiller, $F(1, 194) = 4.94$, $p = .027$, $\eta_p^2 = .025$; consistent with the finding in Study 2a, those in the ingroup condition ($M = 4.13$, $SD = 1.10$) had significantly more trust for the surveiller than those in the outgroup condition, ($M = 3.79$, $SD = 1.09$). The main effect of accuracy, $F(2, 194) = 0.28$, $p = .760$, $\eta_p^2 = .003$, and the interaction, $F(2, 194) = 0.87$, $p = .421$, $\eta_p^2 = .009$, were both non-significant.

The role of trust: Does surveiller identity predict group-based recognition and privacy concern through trust? In Study 2a, we tested an indirect path between surveiller identity and psychological outcomes via trust. Here, a main effect has been established between surveiller identity and trust, and trust is also correlated with the group-based recognition measures and privacy concern. As such, a mediation analysis was conducted using SPSS PROCESS macro (Model 4; Hayes, 2013) for each psychological outcome (Figure 9).

Distinctiveness. Participants felt more trust when surveillance was conducted by the ingroup, compared to when it was conducted by the outgroup, b = -.35, p = .027, SE = .16, 95% CI [-0.65, -0.04]. In turn, greater feelings of trust predicted more perceived distinctiveness, b = .43, p < .001, SE = .06, 95% CI [0.31, 0.55]. The indirect effect was also significant, b = -.15, SE = .06, 95% CI [-0.27, -0.01]. A direct effect was also found between group and distinctiveness b = .42, p = .002, SE = .14, 95% CI [0.15, 0.69].

Understanding. Greater feelings of trust predicted more felt understanding, b = .46, p < .001, SE = .06, 95% CI [0.35, 0.57]. The indirect effect was also significant, b = -.16, SE = .07, 95% CI [-0.30, -0.02]. The direct effect of group on distinctiveness was not significant, b = .19, p = .129, SE = .12, 95% CI [-0.05, 0.42].

Positivity. Greater feelings of trust predicted more perceived positivity, b = .38, p < .001, SE = .05, 95% CI [0.28, 0.49]. The indirect effect was also significant, b = -.13, SE = .06, 95% CI [-0.26, -0.01]. The direct relationship between group and positivity approached significance, b = .21, p = .073, SE = .12, 95% CI [-0.02, 0.44].

Privacy concern. More trust predicted less privacy concerns, *b* = -.43, *p* < .001, *SE* = .06, 95% CI [-0.54, -0.31]. The indirect effect was also significant, *b* = .15, *SE* = .07, 95% CI [0.02, 0.29]. A significant direct relationship was found between group and privacy concern, whereby *outgroup* surveillance was associated with *less* privacy concern, *b* = -.30, *p* = .018, *SE* = .12, 95% CI [-0.54, -0.05].

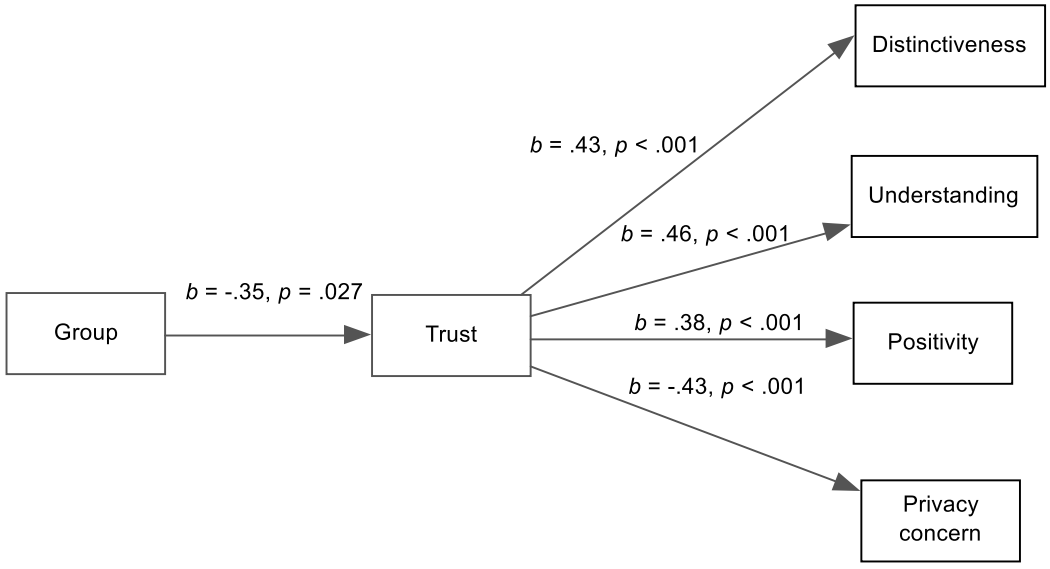


Figure 9. PROCESS path diagram for predicted model. Unstandardised regression coefficients and significance values are presented adjacent to each line that represents the relationship between variables.

Post-hoc analyses: Accuracy *perceptions* as a predictor

Whilst the accuracy manipulation again did not affect any of the psychological outcomes, we can see from Table 5 that accuracy *perceptions* are associated with the recognition dimensions and privacy concern. Additionally, Study 2a found an interaction between accuracy perceptions and surveiller identity on group-based recognition. As with Study 2a, we tested this

interaction with a moderation analysis using PROCESS (Model 1; Hayes, 2013). Surveillance accuracy perceptions were entered as the independent variable and surveiller identity was entered as the moderator on each psychological outcome measure.

Distinctiveness. Significant main effects were found for both surveillance accuracy perceptions, b = .49, se = .067, p < .001, 95% CI [0.353, 0.618], and surveiller identity, b = 0.16, se = .067, p = .020, 95% CI [0.025, 0.289]. Additionally, an interaction was found between surveillance accuracy perceptions and surveiller identity on distinctiveness, b = -.14, se = .067, p = .041, 95% CI [-0.270, -0.006]. Simple slopes analysis revealed that the association between accuracy perceptions and distinctiveness was positive and significant for both the outgroup, b = .35, SE = .094, p < .001, 95% CI [0.163, 0.533], and the ingroup, b = .62, SE = .096, p < .001, 95% CI [0.434, 0.813]. As shown in Figure 10, these results present a different pattern from those found in Study 2a, in that both ingroup and outgroup surveillance were more likely to provide group-based distinctiveness when surveillance was perceived as more accurate.

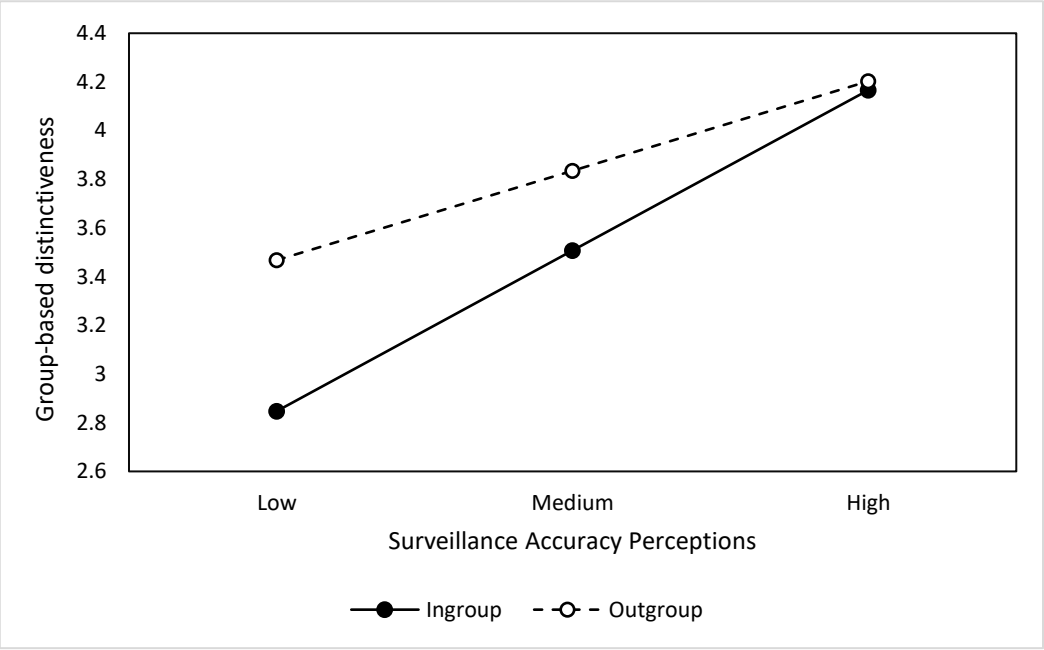


Figure 10. The conditional effect of surveillance accuracy perceptions on perceived distinctiveness at the level of the ingroup and outgroup. Low and high accuracy are valued at 1SD below and above the mean respectively. Medium is valued at the mean.

Understanding. The main effect of accuracy perceptions on felt understanding was significant, b = .38, SE = .065, p < .001, 95% CI [0.255, 0.510], whereby perceiving surveillance as more accurate was associated with more group-based felt understanding. No main effect was found for surveiller identity, b = .03, SE = .065, p = .652, 95% CI [-0.098, 0.156] and no interaction was found between accuracy perceptions and surveiller identity, b = -.0001, SE = .065, p = .999, 95% CI [-0.128, 0.127].

Positivity. A main effect was found of accuracy, whereby perceiving surveillance as more accurate was associated with a greater experience of group-based positivity, b = .37, SE = .060, p < .001, 95% CI [0.249, 0.484], but not of surveiller identity, b = .05, SE = .059, p = .368, 95% CI [-0.064, 0.171].

No interaction was found either, *b* = -.03, *SE* = .060, *p* = .595, 95% CI [-0.149, 0.086].

Privacy concern. A main effect was found of accuracy, whereby perceiving surveillance as more accurate was associated with *less* concern, *b* = -.15, *SE* = .069, *p* = .027, 95% CI [-0.292, -0.018], but not of surveiller identity, *b* = -.08, *SE* = .069, *p* = .244, 95% CI [-0.217, 0.056]. No interaction was found either, *b* = -.01, *SE* = .069, *p* = .924, 95% CI [-0.143, 0.130].

Trust. A main effect was found of surveillance accuracy, *b* = .35, *SE* = .074, *p* < .001, 95% CI [-0.204, 0.495], whereby perceiving surveillance as more accurate was associated with greater trust. Additionally, a significant effect was found of surveiller identity, *b* = -.16, *SE* = .074, *p* = .033, 95% CI [-0.304, -0.013], whereby the outgroup was trusted less than the ingroup. No interaction was found either, *b* = .05, *SE* = .074, *p* = .506, 95% CI [-0.097, 0.195].

Do group-based recognition, privacy concern, and trust predict feelings towards surveillance?

Two multiple regression analyses were conducted to investigate whether privacy concerns, trust, and group-based recognition (positivity, distinctiveness, and understanding) predicted feelings towards surveillance (positive and negative).

Positive feelings towards surveillance. The overall model was significant and explained 47% of the variance (R^2 adj = .47, $F(5, 194) = 36.65$, $p < .001$). Results are presented in Table 6.

Of the recognition measures, positivity predicted positive feelings towards surveillance, as greater perceptions of positivity predicted more positive feelings towards surveillance. Understanding did not uniquely predict positive

feelings towards surveillance and distinctiveness approached significance. Privacy concerns negatively predicted positive feelings towards surveillance, in that more concerns predicted less positive feelings. Trust also predicted feelings towards surveillance, as more trust predicted more positive feelings towards surveillance.

Table 6. Multiple regression analysis investigating the relationship between psychological outcomes and positive feelings towards surveillance

IV	*b*	β	*t*	*p*
Privacy concern	-.16	-.17	-2.88	.004
Distinctiveness	.12	.13	1.92	.057
Understanding	.04	.04	0.55	.582
Positivity	.33	.31	4.87	<.001
Trust	.25	.29	4.28	<.001

Negative feelings towards surveillance*.* The overall model was significant and explained 44% of the variance (R^2 adj = .44, $F(5, 194) = 32.77$, $p < .001$). Results are presented in Table 7.

Trust was the only measure to significantly predict negative feelings towards surveillance, as greater trust predicted less negative feelings towards surveillance.

Table 7. Multiple regression analysis investigating the relationship between psychological outcomes and negative feelings towards surveillance

IV	*b*	β	*t*	*p*
Privacy concern	.09	.09	1.42	.156
Distinctiveness	-.01	-.01	-0.17	.868
Understanding	-.03	-.03	-0.47	.642
Positivity	-.03	-.03	-0.39	.698
Trust	-.55	-.60	-8.69	<.001

Discussion

In this study, we aimed to address two main limitations of Study 2a. Firstly, we argued that the surveillance accuracy manipulation in Study 2a was not strong enough, as accuracy was not related to privacy concern nor group-based recognition. Therefore, in the present study we aimed to include more surveillance accuracy manipulation content in the news bulletin. Additionally, we aimed to include feelings towards surveillance as the primary dependent variable, rather than online behaviour change intentions, as the former was of greater interest to us and would be included in subsequent studies. Study 2b also aimed to replicate the exploratory findings suggesting that trust might mediate the relationship between surveiller identity and psychological outcomes.

Positive pathway: Does accurate surveillance predict more positive (and less negative) feelings towards surveillance through group-based recognition?

The effect of surveillance accuracy and surveiller identity. Whilst Study 2a found an (albeit weak) interaction between surveillance accuracy *perceptions* and surveiller identity on group-based recognition, no consistent interaction was found in Study 2b. Additionally, neither this study nor Study 2a found an interaction between the surveillance accuracy manipulation and surveiller identity on group-based recognition. Instead, both studies suggest greater support for the independent effects of surveillance accuracy perceptions and surveiller identity (through trust).

Surveiller identity (through trust). Participants in the ingroup surveiller condition reported significantly more trust in the surveiller compared to those in the outgroup condition. In turn, greater trust predicted more group-based recognition (on all dimensions). This is consistent with the findings of Study 2a, which also found evidence for an indirect effect of surveiller identity on group-based recognition via trust.

Surveillance accuracy. No main effect was found of surveillance accuracy on group-based recognition. However, surveillance accuracy *perceptions* had a positive association with all three recognition dimensions: those that perceived surveillance as being more accurate were more likely to feel group-based recognition. This supports the findings from Study 2a and provides further correlational evidence for the positive pathway in our model: when surveillance is perceived as accurate, surveillance has the potential to foster positive psychological outcomes in the form of group-based recognition.

The relationship between group-based recognition and feelings towards surveillance. Both distinctiveness and positivity predicted positive feelings towards surveillance. Specifically, greater perceptions of group distinctiveness and positivity was associated with more positive feelings towards surveillance. Whilst this relationship has not been explored in psychological research on surveillance, it is consistent with research in marketing that demonstrates that individuals have a preference for marketing surveillance when it is identity relevant. Specifically, individuals typically prefer targeted advertising when the promoted products or services correspond to their attitudes and beliefs (Campbell & Wright, 2008; McDonald & Cranor, 2010; Ur et al., 2012). The current study illustrates that identity-relevant surveillance may also be preferred outside of advertising contexts. As a result, whilst most advertising literature argues that identity-relevant surveillance is preferred due to its utility for consumers (e.g., financial discounts), this study demonstrates that surveillance that provides group-based recognition may have an intrinsic value, over and above potential material gains.

None of the group-based recognition dimensions uniquely predicted negative feelings towards surveillance. Thus, it could be argued that feeling more group-based recognition may not negate negative feelings towards surveillance, nor does less group-based recognition increase negative feelings towards surveillance. However, a more likely explanation is that the group-based recognition items do not have unique predictive power, and the effects of each are cancelled out when entered together. This is evidenced by the zero-order correlations; all the group-based recognition dimensions correlated (in the predicted direction) with negative feelings towards surveillance, i.e., more group-based recognition was correlated with less negative feelings towards

surveillance. As such, the three dimensions taken together may have cancelled out the effects of one another.

Negative pathway: Does accurate surveillance predict less positive (and more negative) feelings towards surveillance through privacy concern?

The effect of surveillance accuracy and surveiller identity. No interaction was found between surveillance accuracy and surveiller identity on privacy concern. Additionally, no interaction was found between accuracy *perceptions* and surveiller identity. As with the positive pathway, surveillance accuracy perceptions and surveiller identity (through trust) appeared to have independent associations with privacy concerns.

Surveiller identity (through trust). Before addressing the mediation findings, it is important to note that our results for a direct relationship between surveiller identity and privacy concern demonstrated suppression effects. When tested with a MANOVA we did not find evidence for a direct effect; however, a direct relationship was found when conducted in PROCESS when controlling for trust. This direct relationship was in the opposite direction to what was expected: outgroup surveillance was associated with *less* privacy concern. Suppression effects can occur when direct and indirect effects are in opposite directions. Here, it could be that outgroup surveillance is seen as less consequential than ingroup surveillance. When surveilled by an ingroup there is a degree of intragroup accountability, where group members may be punished if they are not conforming to group norms (Goette, Huffman, & Meier, 2006; McLeish & Oxoby, 2007). As such, ingroup surveillance may be associated with more privacy concern (direct path). However, our findings demonstrate that ingroup surveillance may simultaneously be associated with *less* privacy

concern because the ingroup is trusted to a greater extent (indirect path). Consequently, when comparing the psychological outcomes of ingroup versus outgroup surveillance it is prudent to include surveiller trust in the model, as findings may differ depending on whether trust is controlled for in the analyses.

Regarding the mediation findings, an ingroup surveiller was trusted to a greater extent than an outgroup surveiller. In turn, greater trust was associated with less privacy concern. This is consistent with Study 2a and prior literature, which finds that ingroup surveillance raises fewer privacy concerns (O'Donnell et al., 2010a). This present study finds further evidence that this relationship is explained by greater trust in an ingroup surveiller.

Surveillance accuracy. As mentioned above, the surveillance accuracy manipulation did not affect privacy concerns. However, surveillance accuracy *perceptions* predicted privacy concern; surveillance of greater accuracy was associated with *less* privacy concern. As Study 2a found *no* association between surveillance accuracy perceptions and privacy concern, further research is required to explore the nature of the potential effects of surveillance accuracy on privacy concern. The relationship between surveillance accuracy perceptions and privacy concern is also tested in Study 2c and Chapters 4 and 5.

The relationship between privacy concern and feelings towards surveillance. Greater privacy concern predicted less positive feelings towards surveillance. There was no association between privacy concern and negative feelings towards surveillance. The latter is not consistent with prior research; for example, participants in Pavone and Esposti's (2010) study found that participants who felt surveillance was an invasion of privacy typically reported

more negative feelings towards surveillance than those who did not perceive it as an invasion of privacy. Additionally, when Oulasvirta et al. (2012) exposed participants to home surveillance, respondents reported heightened privacy concern, which in turn made them feel ‘weirdness’ and ‘annoyance’. However, many reported a reduction in these negative feelings as the study progressed, despite intense feelings of privacy concern. Participants’ negative feelings subsided as they reported ‘getting used to’ and ‘normalizing’ the surveillance (p. 46). It may be that students simply expect a degree of monitoring from the university. Therefore, whilst increased privacy concern predicts less positive feelings towards surveillance, students may not necessarily feel more negatively, as institutional surveillance is something they have grown accustomed to.

Findings summary

In sum, contrary to our predictions we did not find that surveiller identity moderated the effect of surveillance accuracy on group-based recognition. Instead, we found that accuracy (perceptions) and surveiller identity had independent effects. Specifically, perceiving surveillance as more accurate was associated with greater group-based recognition and less privacy concern. Ingroup surveillance was also associated with more group-based recognition and less privacy concern through an increase in trust. Neither group-based recognition nor privacy concern predicted negative feelings towards surveillance, however greater feelings of group-based distinctiveness and positivity predicted more positive feelings and greater privacy concern predicted less positive feelings.

Limitations

It is important to note that Studies 2a and 2b both recruited student samples. In Study 2a a large proportion of the students were recruited whilst in lecture halls before their lecture began. The lecture did not begin until students handed their surveys back to the experimenter (either complete or incomplete). Additionally, in Study 2b participants received an incentive of course credit in exchange for participation. It is quite possible that in both studies students were not motivated to engage with the manipulation material, as they wanted to proceed with their lecture (Study 2a) or accrue course credit before the summer deadline (Study 2b). Additionally, as this was a relatively novel or unfamiliar form of surveillance, students may have been unsure of the consequences of surveillance or may have believed the surveillance was inconsequential. As such, it may not have been evident to students *how* or *if* surveillance of varying accuracy translated to group-based recognition or privacy infringement. Consequently, whilst the manipulation check was successful, the effect of the accuracy manipulation was again weak. This could in turn account for the lack of effect of the surveillance accuracy manipulation on psychological outcomes.

On the other hand, the manipulation of surveiller identity may not have been affected by student engagement in the same way, as this was comparatively clear and concrete information. Surveillance accuracy is arguably more nuanced and abstract, and therefore the effect of any manipulation may be more vulnerable to (lack of) participant engagement or understanding. This is in line with the concreteness effect, whereby concrete information is typically processed more efficiently (and is less vulnerable to decay) than abstract information (Jessen et al., 2000). Therefore, participants' potential lack of engagement may have weakened the surveillance accuracy manipulation.

STUDY 2C

As such, Study 2c recruited a non-student demographic, where participation was not compensated nor incentivised. Additionally, we changed the context of surveillance in Study 2c to government surveillance (American vs British). By doing this we hoped that the consequences of surveillance may be more familiar and that participants would be more likely to engage with the study materials.

The role of surveiller identity and surveillance accuracy differed between the findings in Study 2a and 2b. In Study 2a we found evidence that surveiller identity may moderate the relationship between surveillance accuracy *perceptions* on group-based recognition. However, surveiller identity did not moderate the effect of the surveillance accuracy manipulation on group-based recognition. Additionally, Study 2b did not find that surveiller identity moderated the association between surveillance accuracy (nor accuracy perceptions) on group-based recognition. Instead, Study 2b found that surveillance accuracy and surveiller identity had independent effects on group-based recognition. As such, in Study 2c we tested our predicted model in a non-student sample to test between the possible interactive or independent effects of the independent variables. Whilst we predicted interactive effects between surveiller identity and surveillance accuracy on group-based recognition in Studies 2a and 2b, the results from these studies led us to predict direct (and non-interactive) effects on group-based recognition in Study 2c.

We also found a relationship between surveillance accuracy perceptions and privacy concern in Study 2b, but not 2a. Study 2c further tested the relationship between surveillance accuracy, accuracy perceptions, and privacy

concern. Additionally, Study 2b found no association between psychological outcomes (group-based recognition and privacy concern) and negative feelings towards surveillance. In Study 2c, we further tested whether group-based recognition and privacy concern are more strongly associated with positive feelings towards surveillance than negative feelings. We also aim to replicate the findings from Study 2a and 2b, whereby outgroup surveillance was associated with less group-based recognition and more privacy concern through a reduction in surveiller trust.

To test our predictions, we recruited British participants from the general population via snowball sampling online. Similar to the design in Study 1, participants were asked to read a news article ostensibly from *Wired*. The article described surveillance conducted by either the NSA (outgroup) or GCHQ (ingroup). The accuracy of the surveillance was described as being of low, medium, or high accuracy. Participants were then directed to the survey containing the dependent measures.

Method

Participants and design

Participants were recruited through opportunistic sampling using social media platforms accessible to the researchers. A total of 489 submissions were recorded, however 245 participants were not included in the analyses as they had at least one dependent measure without any response[17]. This left 244 participants. A majority of 58% were women (40% men, 2% non-binary or prefer not to say) and 76% identified as being White (8% Mixed, 12% Asian, 3% Black,

[17] Participants were excluded if they had at least one dependent measure with no response, as complete data was required for CFA. Missing data treatment could not be conducted if a measure had zero response.

1 Arab, 1% Other). Participants had a mean age of 27.74 years (*SD* = 12.81). A sensitivity analysis using g*power indicated that a sample of 244 is sufficient to detect an effect size using MANOVA of $f = 0.20$ ($\eta_p^2 = .19$) with 80% power for the main effects of and interaction between surveillance accuracy and surveiller identity (two predictors; six groups). When using regression (five predictors), the current study is sufficient to detect an effect size of $f = 0.18$ (partial $r = .18$) with 80% power for each of the effects of distinctiveness, understanding, positivity, privacy concern, and trust.

As in studies 2a and 2b, the study had a 3 (accuracy: low, medium, high) X 2 (group: ingroup, outgroup) between-participants design and participants were assigned randomly to one of the six conditions. Feelings towards surveillance was included as the dependent variable, which was divided into positive and negative feelings towards surveillance. Mediators included perceived group-based recognition (distinctiveness, positivity, and understanding), trust, and privacy concern.[18]

Measures

Unless otherwise stated, responses were collected using a 7-point scale (1 = *Strongly disagree* to 7 = *Strongly agree*). Negatively phrased items were reverse coded.

Identity salience. Participants were asked to write three things that they felt made British people different from other nationalities (based on Haslam et al., 1999). This was included to ensure participants' British identity was salient at the time of completing the survey.

[18] Additional measures were also taken but not included in the analyses. All measures may be found in Appendix I.

Identification. The 4-item identification scale from Study 2b was modified for the context of this study. Items included 'I identify with other British people' and 'I am glad to be British'. All items were used for the final identification scale (α = .85 *M* = 5.24; *SD* = 1.14).

Manipulation. Participants were then asked to read an article ostensibly from *Wired* (Appendix H). Six versions of the article were created, in which both surveillance accuracy and surveiller identity was manipulated. As before, surveillance accuracy was manipulated to have three levels: low, medium, and high; and accuracy manipulation information was included in all but one paragraph within the article. Particular reference to accuracy was on occasion highlighted with blue text (this type of formatting for emphasis is also common within genuine *Wired* publications). Examples include, 'Our analyses suggest that the data collected by (GCHQ/NSA) is *highly representative* of the British Population' (high accuracy), 'Our analyses suggest that the data collected by (GCHQ/NSA) provides a *slightly blurred* impression of the British Population' (medium accuracy), and 'Our analyses suggest that the data collected by (GCHQ/NSA) is *not at all* representative of the British population' (low accuracy). To manipulate surveillance surveiller identity, surveillance was described as being conducted by either British intelligence (ingroup) or American intelligence (outgroup). A picture of GCHQ or the NSA was included to reinforce the surveiller identity manipulation.

Dependent measures. ***Accuracy manipulation check.*** Two items assessed the effectiveness of the accuracy manipulation ('The *Wired* article suggests that algorithmic surveillance is…', 'After reading the article, in my opinion algorithmic surveillance is…). Responses were measured on a 7-point

Likert scale (1 = *Not at all accurate* to 7 = *Extremely accurate*). The two items were averaged to create the final scale (*r* = .65, *M* = 3.97; *SD* = 1.63).

***Perceived group-based recognition*.** As with Study 2b, the measures of group-based recognition included three dimensions (in contrast to Study 2a, which included a unidimensional measure of group-based recognition): positivity, distinctiveness, and understanding. To test our predicted factor structure of group-based recognition a Confirmatory Factor Analysis was conducted (Appendix J). A three-factor solution was supported by CFA.

Positivity. Two items measured how positively people felt British people were perceived by others (e.g. 'The results of algorithmic surveillance by the NSA/GCHQ offers a positive image of British people). Both items were averaged to create the final scale (*r* = .19 *M* = 3.88; *SD* = 0.85).

Distinctiveness. Four items measured the extent to which participants felt surveillance recognised British people as a distinct nationality. Items included 'From using algorithmic surveillance, the NSA/GCHQ recognises that British people have distinct characteristics'. All four items were averaged to create the final scale (α = .42, *M* = 4.10; *SD* = 0.82[19]).

Understanding. To measure the extent to which participants felt surveillance would allow others to understand ingroup members, four items were included such as 'Algorithmic surveillance helps the NSA/GCHQ understand British cultural values'. All four items were used to create the final scale (α = .80, *M* = 3.44; *SD* = 1.19).

[19] Whilst scale reliability was poor, we retained all items to preserve the a priori scale structure.

***Feelings towards surveillance*.** Identical to Study 2b, feelings towards surveillance was measured with two scales: positive emotion and negative emotion. Participants were asked, 'Algorithmic surveillance makes me feel…' and were then presented with 14 emotion items (seven items per scale).

Positive emotion. All seven items, such as 'happy' and 'pleased' were averaged to form the positive emotion scale (α = .93, *M* = 2.94; *SD* = 1.09).

Negative emotion. All seven items, such as 'angry' and 'anxious' were averaged to create the negative emotion scale (α = .90, *M* = 4.28; *SD* = 1.11).

Trust. To measure the extent to which participants trusted the source of surveillance, four items were included, such as 'I trust the NSA/GCHQ to gather British people's online data'. All items were averaged to form the final scale (α = .85, *M* = 3.35; *SD* = 1.27).

Privacy concern. Four items measured the extent to which participants felt surveillance compromised their privacy. Items included 'Surveillance online is an invasion of privacy' and 'people have a right to use the internet without being surveilled'. All items were used to create the final scale (α = .76, *M* = 4.78; *SD* = 1.19).

Demographics. Participants were asked to provide their age, gender, and ethnicity. They were also asked how long they spent online, whether they belonged to closed/private groups online, and how aware they were of surveillance online (1 = *Not at all aware* to 10 = *Very aware*).

Procedure

Participants were recruited on social media platforms, such as Facebook and Twitter. Participants were presented with a brief description of the study

before continuing to the consent form. On giving their informed consent, participants completed the pre-manipulation measures before being randomly allocated to one of the six conditions. They were then asked to read the article corresponding to their condition before completing the dependent measures. On completion or withdrawal, participants were thanked, fully debriefed, and provided with online sources pertaining to internet privacy online should they feel concerned.

Results

Missing data treatment

Analysis of missing data revealed that only 0.2% of values were missing across all measures. Missing values were imputed using the expectation-maximisation (EM) method in SPSS (Graham, 2009) and estimated values fell within the scale range.

Manipulation check

A two-way analysis of variance (ANOVA) was conducted to assess whether the level of surveillance accuracy reported in the article and the surveiller's identity affected perceived surveillance accuracy. There was a significant effect of surveillance accuracy on perceived accuracy of surveillance $F(2, 238) = 126.60$, $p < .001$, $\eta_p^2 = .515$ – a notably stronger effect than was observed in studies 2a or 2b. Pairwise comparisons revealed that those in the high accuracy condition ($M = 5.56$, $SD = 1.18$) reported higher accuracy perceptions than those in the medium accuracy condition ($M = 3.28$, $SD = 1.06$; $p < .001$). Those in the medium accuracy condition reported marginally significantly greater accuracy perceptions than those in the low accuracy condition ($M = 3.00$, $SD = 1.18$; $p = .084$). Consequently, the manipulation was considered successful. No main effect was found of surveiller identity $F(1, 238)$

= 0.02, p = .880, η_p^2 < .001, nor an interaction, $F(2, 238) = 0.42$, p = .660, η_p^2= .003. Correlations between all dependent measures may be found in Table 8.

Table 8. Correlations between measures

Variable	1.	2.	3.	4.	5.	6.	7.
1. Accuracy perceptions	-						
2. Negative feelings	-.04	-					
3. Positive feelings	.12	-.51***	-				
4. Trust	.21**	-.40***	.55***	-			
5. Privacy concern	.03	.45***	-.39***	-.45***	-		
6. Distinctiveness	.36***	.05	.06	.14*	.11	-	
7. Understanding	.48***	-.18**	.27***	.39***	-.07	.27	-
8. Positivity	.16*	-.27***	.29***	.29***	-.25***	.11	.25***

Note. *p < .05, **p < .01, ***p < .001.

Main analyses

Feelings towards surveillance. A multivariate analysis of variance (MANOVA) was conducted with surveillance accuracy and surveiller identity as fixed factors. Positive emotion and negative emotion were entered as dependent variables. The multivariate main effect of surveiller identity approached significance, Wilks' Lambda = .98, F = 2.90, p = .057, η_p^2 = .024. A significant multivariate main effect was found of surveillance accuracy, Wilks' Lambda = .94, F = 3.47, p = .008, η_p^2 = .028. There was no evidence of a multivariate interaction between surveillance accuracy and surveiller identity, Wilks' Lambda = .99, F = 0.92, p = .453, η_p^2 = .008.

Positive feelings. A significant main effect of surveiller identity was found on positive feelings towards surveillance, $F(1, 238) = 4.01$, $p = .046$, $\eta_p^2 = .017$: those in the ingroup condition ($M = 3.09$, $SD = 1.11$) had more positive feelings towards surveillance than the outgroup condition ($M = 2.81$, $SD = 1.07$). The main effect of surveillance accuracy, $F(2, 238) = 0.58$, $p = .561$, $\eta_p^2 = .005$, and the interaction were both non-significant, $F(2, 238) = 1.46$, $p = .235$, $\eta_p^2 = .012$.

Negative feelings. No main effect was found for surveiller identity on negative feelings towards surveillance, $F(1, 238) = 0.01$, $p = .931$, $\eta_p^2 < .001$, but the main effect of surveillance accuracy was significant, $F(2, 238) = 3.13$, $p = .045$, $\eta_p^2 = .026$. Pairwise comparisons revealed that those in the low accuracy condition ($M = 4.41$, $SD = 0.97$) had significantly more negative feelings towards surveillance than those in the medium accuracy condition ($M = 4.02$, $SD = 1.23$, $p = .023$). Additionally, those in the medium accuracy condition had significantly less negative feelings compared to those in the high accuracy condition ($M = 4.40$, $SD = 1.09$, $p = .032$). There was no difference in negative feelings between those in the low and high accuracy conditions ($p = .946$). The interaction was not significant, $F(2, 238) = 0.46$, $p = .635$, $\eta_p^2 < .004$.

Positive psychological outcomes: Group-based recognition. A second MANOVA was conducted with surveillance accuracy and surveiller identity as fixed factors. Distinctiveness, positivity, and understanding were entered as dependent variables. The multivariate main effect of surveiller identity was not significant, Wilks' Lambda = .99, $F = 1.16$, $p = .326$, $\eta_p^2 = .015$. A significant multivariate main effect was found for surveillance accuracy, Wilks' Lambda = .82, $F = 8.10$, $p < .001$, $\eta_p^2 = .093$. There was no indication of a

multivariate interaction between surveillance accuracy and surveiller identity, Wilks' Lambda = .99, $F = 0.47$, $p = .831$, $\eta_p^2 = .006$.

Distinctiveness. The main effect of surveiller identity was not significant, $F(1, 238) = 0.38$, $p = .540$, $\eta_p^2 = .002$, but the main effect of accuracy was significant $F(2, 238) = 8.75$, $p < .001$, $\eta_p^2 = .068$. Pairwise comparisons revealed that those in the low accuracy condition ($M = 3.95$, $SD = 0.86$) did not significantly differ in distinctiveness compared to those in the medium accuracy condition ($M = 3.94$, $SD = 0.72$, $p = .936$). However, those in the medium accuracy condition reported significantly less perceived distinctiveness than those in the high accuracy condition ($M = 4.39$, $SD = 0.79$, $p < .001$). Additionally, those in the high accuracy condition reported significantly more perceived distinctiveness than those in the low accuracy condition ($p < .001$). The interaction was not significant, $F(2, 238) = 0.44$, $p = .645$, $\eta_p^2 = .004$.

Understanding. The main effect of surveiller identity was not significant, $F(1, 238) = 2.37$, $p = .125$, $\eta_p^2 = .010$, but the main effect of accuracy was significant, $F(2, 238) = 17.59$, $p < .001$, $\eta_p^2 = .129$. Pairwise comparisons revealed that those in the low accuracy condition ($M = 2.91$, $SD = 1.08$) reported significantly less felt understanding than those in the medium accuracy condition ($M = 3.45$, $SD = 1.00$, $p = .003$). Additionally, those in the medium accuracy condition reported significantly less felt understanding than those in the high accuracy condition ($M = 3.93$, $SD = 1.19$, $p = .006$). Finally, those in the high accuracy condition reported significantly more felt understanding than those in the low accuracy condition ($p < .001$). The interaction was not significant, $F(2, 238) = 0.67$, $p = .515$, $\eta_p^2 = .006$.

Positivity. No main effect was found for surveiller identity on positivity, $F(1, 238) = 0.02$, $p = .882$, $\eta_p^2 < .001$, but the main effect of surveillance

accuracy was significant, $F(2, 238) = 4.39$, $p = .013$, $\eta_p^2 = .036$. Pairwise comparisons revealed that those in the low accuracy condition ($M = 3.65$, $SD = 0.97$) reported significantly less perceived positivity than those in the medium accuracy condition ($M = 4.01$, $SD = 0.77$, $p = .008$). Those in the medium accuracy condition did not differ in perceived positivity compared to those in the high accuracy condition ($M = 3.97$, $SD = 0.76$, $p = .793$). Those in the high accuracy condition reported significantly more perceived positivity than those in the low accuracy condition ($p = .015$). No significant interaction was found, $F(2, 238) = 0.41$, $p = .667$, $\eta_p^2 = .003$.

Privacy concern and trust. A third MANOVA was conducted with surveiller identity and surveillance accuracy as fixed factors and privacy concern and trust as dependent variables. The multivariate main effect of surveiller identity was significant, Wilks' Lambda = .83, $F = 24.15$, $p < .001$, $\eta_p^2 = .169$. A significant multivariate main effect was also found for surveillance accuracy, Wilks' Lambda = .94, $F = 3.54$, $p = .007$, $\eta_p^2 = .029$. There was no indication of a multivariate interaction between surveillance accuracy and surveiller identity, Wilks' Lambda = .98, $F = 1.52$, $p = .196$, $\eta_p^2 = .013$.

Privacy concern. No main effect was found of surveiller identity, $F(1, 238) = 0.65$, $p = .420$, $\eta_p^2 = .003$, nor of accuracy, $F(2, 238) = 1.46$, $p = .234$, $\eta_p^2 = .012$, and no interaction was found, $F(2, 238) = 0.04$, $p = .958$, $\eta_p^2 < .001$.

Trust. A main effect was found of surveiller identity, $F(1, 238) = 41.22$, $p < .001$, $\eta_p^2 = .148$. Pairwise comparisons revealed that those in the ingroup condition ($M = 3.85$, $SD = 1.28$) reported significantly more trust than those in the outgroup condition ($M = 2.89$, $SD = 1.09$). The main effect of accuracy was marginally significant $F(2, 238) = 2.85$, $p = .060$, $\eta_p^2 = .023$. Pairwise comparisons revealed that those in the low accuracy condition ($M = 3.23$, $SD =$

1.15) did not differ in trust compared to those in the medium accuracy condition (*M* = 3.22, *SD* = 1.17, *p* = .893). Those in the medium accuracy condition had significantly less trust than those in the high accuracy condition (*M* = 3.57, *SD* = 1.44, *p* = .036), and those in the high had significantly more trust for the surveiller than those in the low (*p* = .047). No interaction between surveiller identity and accuracy was found, $F(2, 238) = 2.01$, $p = .130$, $\eta_p^2 = .017$.

The role of trust: Does surveiller identity predict recognition and privacy concern *through* trust? We also tested the indirect effect of surveiller social identity on recognition and privacy concerns via trust in a mediation analysis using the SPSS PROCESS macro (Model 4; Hayes, 2013) for each outcome.

Distinctiveness. Figure 11 illustrates that participants felt more trust when surveillance was conducted by the ingroup, compared to when it was conducted by the outgroup, *p* < .001, *SE* = .15, 95% CI [-1.26, -0.67]. In turn, greater feelings of trust predicted more perceived distinctiveness, *p* = .008, *SE* = .04, 95% CI [0.03, 0.20]. The indirect effect was also significant, *b* = -.11, *SE* = .04, 95% CI [-0.22, -0.03]. The direct effect of surveiller identity on distinctiveness was not significant, *b* = .18, *p* = .115, *SE* = .11, 95% CI [-0.04, 0.40].

Understanding. Greater feelings of trust predicted more felt understanding, *p* < .001, *SE* = .06, 95% CI [0.27, 0.50] and the indirect relationship was significant, *b* = -.37, *SE* = .08, 95% CI [-0.54, -0.22]. No evidence was found for a direct relationship between surveiller identity and distinctiveness *b* = .15, *p* = .339, *SE* = .15, 95% CI [-0.15, 0.45].

Positivity. Greater feelings of trust predicted more perceived positivity, *p* < .001, *SE* = .04, 95% CI [0.14, 0.31], and a significant indirect relationship was

found, *b* = -.22, *SE* = .06, 95% CI [-0.34, -0.12]. A significant direct relationship was found between surveiller identity and positivity, whereby outgroup surveillance predicted more perceived positivity than the ingroup, *b* = .22, *p* = .049, *SE* = .11, 95% CI [0.00, 0.45].

Privacy concern. More trust predicted less privacy concerns, *p* < .001, *SE* = .06, 95% CI [-0.59, -0.36]. The indirect effect was also significant, *b* = .46, *SE* = .09, 95% CI [0.29, 0.63]. A significant direct relationship was found between surveiller identity and privacy concern, whereby outgroup surveillance predicted less privacy concern, *b* = -.33, *p* = .026, *SE* = .15, 95% CI [-0.62, -0.04].

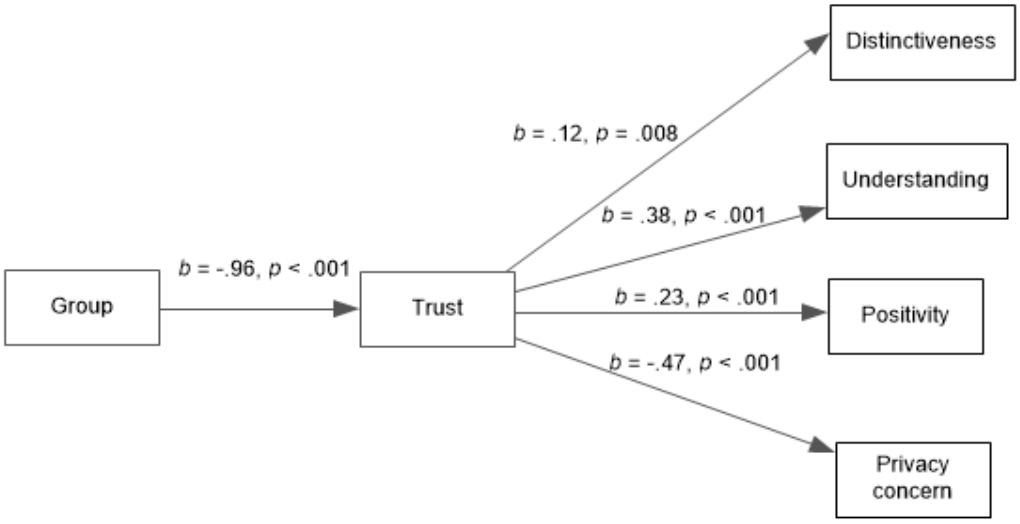


Figure 11. PROCESS path diagram for predicted model. Unstandardised regression coefficients and significance values are presented adjacent to each line that represents the relationship between variables.

Psychological outcomes on feelings towards surveillance. Two multiple regression analyses were conducted to investigate whether privacy concerns, trust, and group-based recognition (positivity, distinctiveness, understanding) predicted feelings towards surveillance (positive and negative).

Positive feelings towards surveillance. The overall model was significant and explained 33% of the variance (R^2 adj = .33, $F(5, 238) = 25.13$, $p < .001$). Results are presented in Table 9.

Of the recognition measures, only positivity uniquely (but marginally) predicted positive feelings towards surveillance, as greater perceptions of positivity predicted more positive feelings towards surveillance. Privacy concerns negatively predicted positive feelings towards surveillance, in that more concerns predicted less positive feelings. Trust also predicted positive feelings towards surveillance, as more trust predicted more positive feelings towards surveillance.

Table 9. Multiple regression analysis investigating the relationship between psychological outcomes and positive feelings towards surveillance

IV	*b*	β	*t*	*p*
Privacy concern	-.16	-.17	-2.82	.005
Distinctiveness	-.01	-.01	-.15	.879
Understanding	.07	.07	1.20	.231
Positivity	.14	.11	1.96	.051
Trust	.36	.41	6.35	<.001

Negative feelings towards surveillance. The overall model was significant and explained 26% of the variance (R^2 adj = .26, $F(5, 238) = 17.87$, $p < .001$). Results are presented in Table 10.

Results mirrored those of positive emotion. Positivity was the only recognition dimension to uniquely predict negative feelings towards surveillance, as greater perceptions of positivity predicted less negative feelings towards surveillance. Privacy concerns positively predicted negative feelings towards surveillance, in that more concerns more negative feelings. Trust also predicted feelings towards surveillance; more trust predicted less negative feelings towards surveillance.

Table 10. Multiple regression analysis investigating the relationship between psychological outcomes and negative feelings towards surveillance

IV	*b*	β	*t*	*p*
Privacy concern	.92	.31	4.87	<.001
Distinctiveness	.10	.08	1.30	.196
Understanding	-.07	-.07	-1.13	.259
Positivity	-.16	-.12	-2.07	.039
Trust	-.18	-.21	-3.00	.003

Discussion

In this study we aimed to improve participant engagement by recruiting a non-Psychology student sample in a more broadly-applicable context (national security surveillance). In turn, we hoped that the surveillance accuracy

manipulation would be stronger and have a greater effect on group-based recognition and privacy concerns. We also used government (rather than university) surveillance as the context for the study, as this context may be more consequential and generalisable to wider society.

A positive pathway: Surveillance accuracy and surveiller identity affects feelings towards surveillance through recognition

More accurate surveillance is associated with more group-based recognition. Study 2c is the first of this chapter to clearly establish an effect of surveillance accuracy on group-based recognition. Whilst Studies 1, 2a and 2b demonstrated a relationship between surveillance accuracy *perceptions* and recognition, the current study demonstrates that surveillance accuracy can directly increase positive psychological outcomes in the form of group-based recognition. One implication of this is that for an association to be found between surveillance accuracy and recognition, identity concerns must be made salient (in this case through an intergroup context) and participants must be appropriately engaged with the study materials for the nuance of a surveillance accuracy manipulation to have a sufficient effect.

Additionally, Study 2c finds greater support for the independent (rather than interactive) effects of surveiller identity and surveillance accuracy on group-based recognition: surveillance of greater accuracy led to greater feelings of distinctiveness, positivity, and understanding; and ingroup (vs. outgroup) surveillance led to more group-based recognition (through trust).

The current study also clearly further underlines the role of trust in intergroup surveillance contexts. We have replicated the mediating effect of trust between surveiller identity and group-based recognition. Participants

reported greater trust when the surveiller was described as ingroup (GCHQ) compared to when the surveiller was identified as outgroup (the NSA). In turn, greater trust was associated with more perceived group-based recognition, in the form of distinctiveness, positivity, and understanding.

Being perceived more positively predicts more positive and less negative feelings towards surveillance. The more individuals felt their group was perceived positively as a result of surveillance, the more positively and less negatively they felt towards surveillance. Positivity was the only recognition dimension to uniquely predict feelings towards surveillance. Distinctiveness and understanding were not significantly associated with feelings towards surveillance in the regression model, however understanding correlated with both positive and negative feelings.

A negative pathway: Surveillance accuracy and surveiller identity affects feelings towards surveillance through privacy concern

Surveiller identity (but not surveillance accuracy) affects privacy concern. Mirroring the findings from Studies 2a and 2b, surveillance accuracy was not associated with privacy concern and no interaction was found between surveillance accuracy and group on privacy concern. However, as demonstrated in Studies 2a and 2b, there was evidence that trust mediated the relationship between surveiller identity and privacy concern. Ingroup surveillance was associated with more trust, which in turn predicted less privacy concern. This supports previous work by O'Donnell et al. (2010a), who found that surveillance from an ingroup elicited less privacy concern than surveillance from a superordinate group. In their work, the appraisal of surveillance as being for the purpose of safety mediated this effect. As the current study used the

context of government surveillance, it could be argued that ingroup surveillance was associated with more trust because it is assumed to be for the benefit of the group (safety), whereas individuals may interpret outgroup surveillance as an effort to control the ingroup (O'Donnell et al., 2010a). In addition to surveillance appraisal, the current study suggests that the association between surveiller identity and privacy concern may also be explained by trust in the surveiller.

The relationship between privacy concern and feelings towards surveillance. Privacy concerns in turn predicted less positive and more negative feelings towards surveillance. This differs slightly from Study 2b, which found an association between privacy concerns and positive feelings towards surveillance, but not negative.

Summary

Of the three studies in this chapter, the current study is the first to demonstrate the predicted causal effect of surveillance accuracy on group-based recognition. We found that greater surveillance accuracy led to a greater perception of group-based recognition. However, group-based recognition dimensions did not have unique predictive effects on feelings towards surveillance, contrary to our expectations. Additionally, we did not find the expected effect of surveillance accuracy on privacy concern. Nevertheless, privacy concern did predict feelings towards surveillance in the expected way: greater privacy concerns were associated with less positive and more negative feelings towards surveillance.

GENERAL DISCUSSION

The studies in this chapter aimed to replicate the findings from Study 1, whilst addressing some key limitations. Specifically, Study 1 provided evidence for the expected negative pathway, whereby more accurate surveillance was associated with more negative feelings towards surveillance through increased privacy concern – although the expected linear trend was only found for higher internet users between medium and high levels of accuracy. However, Study 1 did not provide evidence for the predicted countervailing positive pathway, whereby more accurate surveillance is associated with more positive feelings towards surveillance through increased recognition.

Importantly, Study 1 also did not test our predicted model in the context of *social* identity. We argued that the lack of association between surveillance accuracy and recognition in Study 1 may have been due to the fact that no specific social identity was made salient to participants and recognition referred to individual-based rather than group-based recognition. In each of Studies 2a-2c, we therefore made a social identity salient using an intergroup context, meaning that each study tested the effect of surveillance accuracy on group-based recognition when social identity concerns were salient. We predicted that surveillance accuracy would affect group-based recognition, particularly when the surveiller belonged to a relevant outgroup. Outgroup members are assumed to endorse negative meta-stereotypes (Finkelstein at al., 2013; Sigelman & Tuch, 1997; Vorauer et al., 1998), and are thus unlikely to be perceived as providing group-based recognition. Surveillance of greater accuracy may provide a vehicle for recognition when the surveiller is an outgroup, as baseline group-based recognition may be low. In contrast, group-based recognition is assumed from an ingroup surveiller, as recognition is implied through shared

group membership (individuals are less likely to believe ingroup members endorse negative stereotypes and/or attitudes towards the ingroup; Finkelstein at al., 2013; Sigelman & Tuch, 1997; Vorauer et al., 1998). In turn, greater group-based recognition was assumed to predict more positive feelings towards surveillance.

The positive pathway: More accurate surveillance is associated with more positive feelings towards surveillance through group-based recognition

Surveillance accuracy and surveiller identity on group-based recognition. ***Surveillance accuracy.*** A key aim of these studies was to make social identity concerns salient, and therefore strengthen the potential association between surveillance accuracy and group-based recognition. Indeed, the accuracy manipulation affected (Study 2c) and accuracy perceptions predicted (Study 2b) all three group-based recognition dimensions: the more accurate surveillance was described or perceived to be, the more distinct, positive, and understood participants felt their ingroup was. This suggests that irrespective of the surveiller's identity, when surveillance is accurate it has the potential to increase group-based recognition.

Previous research has suggested that personal/individual recognition may be achieved from accurate social-veillance (i.e. surveillance from other internet users). For example, individuals report feelings of personal recognition when they are accurately perceived by their online blog readership (de Laat, 2008) and friends on social media platforms (Steeves & Bailey, 2016). The three studies presented in this chapter extend this research in several ways. Firstly, we demonstrate that group-based recognition is possible when one is perceived accurately by a relatively abstract (group) source, rather than identifiable internet users. This suggests that individuals only need to be believe

that their data will be assessed accurately by someone/something at some point in time for the potential to achieve group-based recognition. Therefore, as long as surveillance is accurate, direct contact may not be necessary to receive group-based recognition benefits.

Secondly, by manipulating surveillance accuracy directly we highlight that having our personal data visible *per se* is not necessarily enough to foster group-based recognition. To achieve recognition, an individual must believe that their data are being processed accurately and that assumptions based on that data are also accurate. Indeed, previous literature has highlighted that metastereotypes must be made salient for group-based recognition needs to arise. Van Leeuwen and Täuber (2012) found that participants were more likely to engage in identity management strategies (helping the outgroup) if negative metastereotypes were made salient, compared to a positive metastereotype or no metastereotype. This highlights the importance of *feedback*; being privy to the assumptions made about our data and online behaviour may be necessary to increase group-based recognition. Thus, whilst the presence of surveillance (or an audience more generally) can raise identity-related concerns (Barreto et al., 2003), this chapter illustrates that a degree of feedback (in this case surveillance accuracy) is required for social identity concerns to be assuaged (or further magnified). Additionally, whilst the majority of research cited above relates to personal recognition, we demonstrate that individuals may achieve *group*-based recognition through accurate surveillance.

Surveiller identity: Ingroup surveillance is associated with more group-based recognition via trust. An indirect effect of surveiller identity on group-based recognition *through trust* was consistently found across the three studies. An ingroup surveiller was trusted to a greater extent than an outgroup

surveiller, which in turn predicted greater perceptions of group-based recognition.

As discussed, previous literature suggests that individuals typically assume outgroup members hold negative beliefs about the ingroup (Finkelstein at al., 2013; Sigelman & Tuch, 1997; Vorauer et al., 1998). Our results support prior research, as participants were more likely to experience group-based *mis*recognition from an outgroup surveiller compared to an ingroup surveiller. Ingroup surveillance on the other hand was associated with more group-based recognition, as recognition may be implied through shared group membership. Our findings also build upon previous research by illustrating that individuals may assume negative or inaccurate metastereotypes because the outgroup is afforded less trust than an ingroup audience. Consequently, as an ingroup surveiller is afforded more trust, they may be assumed to manage and interpret personal data in a way that recognises the group's identity.

It could be argued that distrust and assumed misrecognition from an outgroup surveiller is due to the expectation that the outgroup may mishandle or manipulate ingroup data. When under outgroup surveillance personal data could be used to embolden pre-existing negative stereotypes. For example, Brighenti (2007) argues that visibility has two opposing outcomes: recognition or control. She suggests that visibility is sometimes necessary for recognition to occur; for example, those living in poverty and the homeless typically do not have access to public platforms whereby they can challenge misconceptions about their group or curate their own identity. As such, a lack of visibility denies these groups recognition. In other contexts, visibility can be used as a method of control and to further stigmatise a group. In this case, the representation of a

group can be warped through visibility. Brighenti gives the example of the media's representation of migrants as criminals.

Others have highlighted how the supra-visibility of women contributes to their sexualisation and commodification (Dubrofsky & Wood, 2014; Mason & Magnet, 2012; Skeggs, 1999). Our findings also demonstrate that being visible through surveillance can undermine group-based recognition when the surveiller is distrusted. However, our findings also illustrated that misrecognition is not an inevitable consequence of outgroup surveillance: when participants believe that surveillance and data processing is accurate, they experience an *increase* in group-based recognition. As such, outgroup surveillance can foster group-based recognition when it is accurate, despite the outgroup typically being afforded less trust.

Does surveiller identity moderate the effect of surveillance accuracy on group-based recognition? Initially we predicted an interaction between surveiller identity and surveillance accuracy on group-based recognition. We anticipated that ingroup surveillance of varying accuracy would be unlikely to improve group-based recognition, as recognition needs are already met through shared group membership. On the other hand, we predicted that greater surveillance accuracy would be associated with more group-based recognition when the surveiller was an outgroup. Overall, our findings provide greater support for the independent rather than interactive effects of surveillance accuracy and surveiller identity. A moderation effect was only found in Study 2a with accuracy perceptions. In Study 2a we found that greater accuracy *perceptions* were associated with more group-based recognition for outgroup surveillance but not ingroup surveillance. However, we did not replicate this interaction in Study 2b nor Study 2c.

Group-based recognition and feelings towards surveillance. Results from Studies 2b and 2c were inconsistent regarding the association between group-based recognition and feelings towards surveillance. In Study 2b, two of the three recognition dimensions (distinctiveness and positivity) predicted positive feelings towards surveillance (distinctiveness was marginally significant). None of the recognition dimensions predicted negative feelings towards surveillance when adjusting for one another and for privacy concern and trust. In Study 2c, only positivity predicted positive and negative feelings towards surveillance. Therefore, the relationship between positivity and positive feelings towards surveillance was the only consistent finding across the two studies.

One implication of this pattern is that there is a potential ambivalence towards surveillance; positive outcomes of surveillance (e.g., the belief that an ingroup is recognised by surveillance) may increase positive feelings towards surveillance yet not necessarily diminish negative feelings. This echoes Ball (2009), who suggested that individuals may feel a gratification from recognition and exhibitionism online, yet still feel uncomfortable about the scrutiny. However, the suggestion of ambivalence here is tentative, as only two of the three studies included feelings towards surveillance as a DV and results differed between these two studies. As such, results from the other chapters within this thesis must be considered before an assumption of ambivalence is made.

The negative pathway: More accurate surveillance is associated with more negative feelings towards surveillance through privacy concern

Surveillance accuracy and surveiller identity on privacy concern.

Surveillance accuracy. Overall, our results provide weak support for a main effect of surveillance accuracy on privacy concern. The studies in this chapter mostly replicated the findings from Study 1, as surveillance accuracy perceptions (but not the accuracy manipulation) were associated with privacy concern in two of the three studies. However, we have argued above that the weak effect of the surveillance accuracy manipulation in Studies 2a and 2b could be attributed to our student samples. As discussed earlier in the chapter, a lack of participant engagement may have reduced the effect of the surveillance accuracy manipulation. To rectify this, in Study 2c we recruited those from the general public and included a more familiar form of surveillance (government intelligence: NSA/GCHQ). Indeed, we found a strong effect of surveillance accuracy in Study 2c. Nevertheless, in Study 2c we still found no effect of the surveillance accuracy manipulation nor surveillance accuracy perceptions on privacy concern. The evidence from the three studies in this chapter does not suggest that surveillance accuracy is associated with privacy concern over and above the mere presence of surveillance. Instead, we found that surveiller identity (discussed below) was a stronger driver of privacy concern.

Surveiller identity: Ingroup surveillance is associated with less privacy concern via trust. We predicted several possible outcomes regarding the effects of surveiller identity on privacy concern. O'Donnell and colleagues have found that ingroup surveillance may be perceived favourably (O'Donnell et al., 2010a) or unfavourably (O'Donnell et al., 2010b) in comparison to outgroup

surveillance. O'Donnell et al. (2010a) argues that surveillance from an ingroup may elicit fewer privacy concerns when it is thought to increase ingroup safety and is therefore considered necessary. Alternatively, surveillance from the ingroup in contexts where it is not considered necessary (e.g., in the workplace) may be perceived negatively (O'Donnell et al., 2012). In light of this, we predicted that surveillance by an ingroup (vs. an outgroup) may be associated with either greater privacy concern, or fewer privacy concerns.

Our findings support the latter with an important caveat: surveillance by an ingroup predicted less privacy concern *through* an increase in trust in all three studies. This is consistent with O'Donnell et al.'s (2010a) findings that surveillance from a sub-group was associated with less privacy concern than surveillance from a superordinate group. However, in O'Donnell and colleagues' study this relationship was explained by surveillance being perceived as safety promoting when conducted by the sub-group (compared to the superordinate group). Indeed, there are numerous studies that demonstrate that the public associate government surveillance with safety, and that safety-promoting surveillance is associated with less concern (Greenwald, 2013; Geiger, 2018).[20] However, O'Donnell et al. (2010a) did not measure surveiller trust in their study, therefore it is unclear whether trust may have played an important role.

Other studies have found that surveiller trust is an integral predictor of concern and attitudes towards surveillance, even when surveillance is safety promoting. Davis and Silver (2004) found that individuals were only willing to exchange their civil liberties for greater security from government surveillance when the government was trusted. Thus, our findings build upon O'Donnell et

[20] However, after the Snowdon leaks in 2013, individuals' felt surveillance went beyond safety and began to encroach on civil liberties, therefore government surveillance was seen as less safety promoting than before the Snowdon leaks (Greenwald, 2013; Geiger, 2018).

al.'s (2010a) results and support Davis and Silver's (2004) study, whereby an organisation (ingroup or outgroup) is not necessarily more likely to elicit privacy concerns per se (irrespective of whether surveillance promotes safety), and the degree to which we trust the group by virtue of whether it is 'us' (ingroup) or 'them' (outgroup) is a critical step in predicting the amount of privacy concern experienced.

Does surveiller identity moderate the effect of surveillance accuracy on privacy concern? We also postulated the possibility that surveiller identity and surveillance accuracy may interact. Surveillance from an outgroup is typically expected (Simon & Oakes, 2006) and therefore participants' privacy concern may be more sensitive to variations in surveillance accuracy when conducted by an outgroup. Additionally, inaccurate surveillance from an outgroup may be associated with more privacy concern, as the motives of the surveiller are assumed to be less positive (Tanis & Postmes, 2005). Surveillance accuracy may not be associated with privacy concern when conducted by the ingroup, as those surveilled may believe data will be used within the group's best interest, irrespective of its accuracy. Alternatively, surveillance from the ingroup may be considered unexpected or unnecessary (O'Donnell et al., 2012) and therefore the mere presence of surveillance may overwhelm the nuance of surveillance accuracy.

Our findings provided no indication of interactive effects between surveillance accuracy and surveiller identity on privacy concern. Instead, surveiller identity's indirect effect through trust was the most consistent predictor of privacy concerns across the three studies in this chapter.

Privacy concerns predict feelings towards surveillance. We expected that greater privacy concerns would in turn predict more negative and less positive feelings towards surveillance. Studies 2b and 2c tested the relationship between privacy concern and feelings towards surveillance. Both studies found that privacy concerns did indeed predict feelings towards surveillance. Study 2b found that greater privacy concerns were associated with less positive (but not more negative) feelings towards surveillance, and Study 2c found that more privacy concern predicted less positive and more negative feelings towards surveillance. This supports previous literature from Pavone and Esposti (2010), who found that those voicing privacy concerns about government surveillance were more likely to feel negatively towards it.

Findings from Study 2b also illustrate the benefit of measuring positive and negative feelings independently, as privacy concern predicted positive and negative feelings in different ways. Whilst these results were not replicated in Study 2c, it suggests that future research should take a similar methodological approach, as this may help highlight contexts in which people feel apathy or ambivalence towards surveillance.

The findings from this Chapter also contribute to the privacy paradox literature. Study 2a found that higher privacy concerns were associated with a greater intention to modify online behaviour. Whilst this was a measure of behavioural *intentions* rather than a direct behaviour measure, it demonstrates that despite research demonstrating no association between privacy concern and privacy-related behaviour, individuals may still have a desire to change their behaviour online. Indeed, some have argued that internet users may not change their online behaviour despite concerns for privacy because they do not know how to (Tene & Polonetsky, 2014) or they may feel social pressure to

continue online engagement (Welinder, 2012). Whilst we did not measure behavioural outcomes, our findings support previous research, whereby internet users may typically feel concerned for their privacy and have a desire to protect it in online spaces.

In sum, the studies in this chapter provide some support for the negative pathway proposed in Chapters 1 and 2. We found evidence that increased privacy concerns predict less positive (and perhaps more negative) feelings towards surveillance. However, we did not find consistent evidence that surveillance accuracy leads to privacy concerns. We did, nevertheless find that the source of surveillance is important in explaining privacy concerns for online users: individuals are more likely to feel greater privacy concern when the surveiller is an outgroup, as the outgroup is trusted less compared to an ingroup surveiller.

Limitations and future research

In all three studies we used contexts in which surveillance could have been appraised as promoting the welfare of the ingroup: participants may have construed university and government surveillance as safety-promoting. As such, future research should endeavour to test our predicted model in a variety of intergroup surveillance contexts in which ingroup surveillance may be less trusted or the outgroup is more trustworthy. For example, surveillance conducted in the workplace may be perceived as within the employers' best interest, rather than the employees (Ball, 2010). As such, (ostensible) ingroup surveillance in this case may be associated with less group-based recognition and more privacy concern, as the surveiller's motive is distrusted.

Additionally, ingroup members who have low identification with the group may experience similar amounts of group-based recognition and privacy concern from ingroup surveillance and outgroup surveillance. Those who do not identify strongly with their ingroup have been shown to trust fellow ingroup members less than those that identify more strongly (Han & Harms, 2010). As trust mediated the relationship between surveiller identity and group-based recognition and privacy concern, low identifiers may experience less group-based recognition benefits and more privacy concern when under ingroup surveillance than those identifying more strongly. These inter/intragroup contexts could be incorporated in future research that tests our proposed model.

Secondly, we did not find the expected interaction between surveiller identity and surveillance accuracy. One possibility is that we did not find this interaction as we did not make meta-perceptions salient in the three studies presented here. Van Leeuwen and Täuber (2012) found that negative group stereotypes must be made salient for impression management strategies to occur. Therefore, a key aim of the final study in this thesis (reported in Chapter 5) was to directly manipulate misrecognition, by exposing participants to either positive or negative stereotypes about their group. We expect that when misrecognition is made salient, individuals will be more likely to receive recognition benefits from accurate surveillance, however surveillance accuracy will have no effect on recognition when individuals feel recognised, as their identity needs are already met.

Summary

The aim of this chapter was to test both the positive and negative pathway in the predicted model. Specifically, we aimed to strengthen the effect

of surveillance accuracy on group-based recognition by making identity concerns salient. We also predicted that this effect would be moderated by the identity of the surveiller. Evidence was found to support the positive pathway, whereby greater surveillance accuracy was associated with more group-based recognition, which in turn predicted more positive feelings towards surveillance.[21] A second positive pathway was found, whereby ingroup surveillance was associated with more trust in the surveiller, and in turn more group-based recognition.

Results partially supported the predicted negative pathway. In all three studies, surveillance accuracy was not associated with privacy concern. However, as expected, privacy concern predicted less positive and (in Study 2c) more negative feelings towards surveillance and stronger behaviour change intentions online (Study 2a). Additionally, a second negative pathway was found via an indirect effect of surveiller identity: outgroup surveillance was trusted less, which in turn predicted greater privacy concern.

In the studies in the next chapter, we built upon these findings by testing the predicted model within different identity-relevant contexts. Whilst the studies in this chapter aimed to raise identity concerns through making an intergroup context salient, the studies in Chapter 4 sought to raise identity concerns by recruiting people from chronically-misrecognised groups: those identifying as gay (Study 3a) and those identifying as vegan (Study 3b). This enabled us to test our predictions within contexts of group-based stigma (unlike those examined in this chapter).

[21] Although it is important to note that positivity was the only group-based recognition dimension to consistently predict feelings towards surveillance.

We also hoped in the following studies to replicate the positive pathway results found in Study 2c, which was the only study thus far to find an effect of the surveillance accuracy manipulation on group-based recognition. [22] Additionally, we aimed to further elucidate the relationship between group based recognition and feelings towards surveillance, as only positivity consistently predicted feelings towards surveillance in Studies 2b and 2c. We also addressed some of the methodological flaws in the studies in this chapter. As such, Chapter 4 did not exclusively recruit students and included those from more diverse demographic backgrounds. Furthermore, our sample sizes in Studies 2a and 2b were restricted to the number of students enrolled in the Psychology undergraduate programme at the time of data collection. Therefore, by recruiting those from the general population we were able to achieve larger sample sizes in both studies included in Chapter 4.

[22] Studies 2a and 2b found a relationship between surveillance accuracy *perceptions* and group-based recognition.

CHAPTER 4

The studies reported in Chapter 3 tested the role of group identity-related concerns in reactions to algorithmic surveillance by manipulating the identity of the surveiller and surveillance accuracy. Chapter 4 takes a different approach; here, we aim to heighten recognition needs by making a stigmatised identity salient. In two studies, we test whether (accurate) algorithmic surveillance provides a vehicle for perceived group-based recognition for those belonging to stigmatised/chronically misrecognised groups, and whether recognition in turn predicts more positive and less negative feelings about surveillance. In keeping with the previous chapters, we also investigated the negative pathway, whereby more accurate surveillance is also expected to raise privacy concerns, which in turn encourages more negative and less positive feelings towards surveillance.

Stigma may be defined as ‘an identity-discrediting mark’ (Meisenbach, 2010, p. 268), whereby an individual or group is ‘disqualified from full social acceptance’ (Goffman, 1963; p. 9). Stigma is not necessarily a static trait. One’s context or environment typically delineates the boundaries of stigma; a group may be considered (unfavourably) different in one context, but not another (Coleman, 1986). As stigma is often imposed on one group from another it has also been described as a communicative process intended to highlight intergroup difference, justify discrimination, and maximise group distinctiveness (Burke, 1969; Coleman, 1986; Falk, 2001).

Belonging to a stigmatised group is associated with negative outcomes. Mental health is often worse for those belonging to stigmatised groups; for example, women who experience greater sexism report more depression and anxiety symptoms than women who experience less sexism (Klonoff, Landrine,

& Campbell, 2000). Additionally, greater feelings of stigma are associated with lower levels of subjective wellbeing (Hutton, Misajon, & Collins, 2012), poorer social health (Doyle & Molix, 2016), and can reduce the quality of romantic relationships (Doyle & Molix, 2014). Stigmatised group members also show reduced performance (in identity relevant domains) compared to majority groups, which may in turn reduce the likelihood that stigmatised groups have equal opportunities for resources and career success (see Steele, Spencer, & Aronson, 2002 for a review). Therefore, belonging to a stigmatised group carries the risk of poorer life outcomes compared to those belonging to majority groups.

To avoid these negative outcomes, members of stigmatised groups often develop strategies to protect their sense of self and to enhance recognition. Indeed, people generally strive for 'individual agency in the process of identity construction' (Harding, 2003; p. 574), yet this is especially true for those with stigma, as the ability to curate one's own identity is difficult or denied altogether (Snow & Anderson, 1987). Past research has described a range of identity-protective strategies that those with stigma employ to reclaim agency over their identity (e.g., Chrobot-Mason, Button, DiClementi, 2001; Miller & Kaiser, 2001). Strategies include disengagement (i.e., downplaying the value or importance of domains in which they experience stigma; Major & Schmader, 1998; Major, Spencer, Schmader, Wolfe, & Crocker, 1998), identity concealment (Newheiser & Barreto, 2014), externalising blame (e.g., blaming negative outcomes on discrimination; Major, Kaiser, & McCoy 2003), and negative stereotype rejection (Luhtanen, 2002).

The employment of identity protective strategies has led some to argue that perceiving group-based stigma can be *protective* against mental illness and

poor self-esteem (e.g., Crocker & Major, 1989; Twenge & Crocker, 2002), as those with stigma become more resilient and empowered through strategies developed and mastered throughout their lives (Shih, 2004). However, others have argued that some strategies can worsen outcomes for stigmatised individuals, as it can impair social interactions and wellbeing (Ilic et al., 2012; Newheiser & Barreto, 2014). Whilst the outcomes of identity-management strategies may vary, this literature demonstrates that those experiencing stigma often seek opportunities to combat its deleterious effects and garner group-based recognition.

We argue that stigmatised individuals may experience algorithmic surveillance as an additional vehicle for recognition. In the case of targeted material online, content will typically try to relate to (and affirm) an important aspect of one's identity. Relevant targeted material is typically received more positively than adverts that do not contain identity-relevant content (Zeng, Huang, & Dou, 2009). The value of identity-relevant content was also demonstrated during the European Union (EU) referendum. For example, the Vote Leave campaign targeted those who supported animal rights with adverts warning of an increase in animal abuse if the United Kingdom remained in the EU (e.g. 'the EU blocks our ability to speak out and protect polar bears! CLICK TO HELP THEM'; 'Vote Leave's targeted Brexit ads released by Facebook', 2018). In this case, those that identified as animal rights activists (or even animal lovers) were provided the opportunity to have a relevant identity recognised in a way that aligned with their own self-concept. Their group membership was accurately identified (subjectively at least) and their needs and interests as a member of that group were in turn recognised. Indeed, this

method of advertising has been argued to have contributed to the referendum result ('Whistle-blower: Brexit vote part of Facebook data scandal', 2018).

However, as discussed in Chapter 1, the potential for group-based recognition through algorithmic surveillance may only exist if surveillance is accurate. If surveillance is not accurate, those living with stigma are likely to experience further misrecognition in addition to what they already experience outside the surveillance context. For example, whilst all travellers are under surveillance in airports, Muslim travellers are often more likely to be categorised as a security threat (Blackwood et al., 2015); for example, Muslims reported that they were more likely to be stopped at airports compared to other travellers, and that they would experience less interference at airports if they dressed in a more stereotypically 'western' way. In this case, the inaccurate assumptions held by those conducting surveillance contributed to feelings of misrecognition for Muslim travellers.

The variability of surveillance accuracy is also evident online. Cinnamon (2017) argues that corporations commonly make inaccurate judgements about individuals based on their online profiles. For example, when assessing financial reliability, individuals can be placed into 'risk' categories which 'produce new social categories of difference and restrict our ability to shape our own sense of self' (p. 616). Therefore, whilst *accurate* algorithmic surveillance may afford stigmatised groups an opportunity for group-based recognition, less accurate surveillance may not provide the same recognition benefits and may instead further misrecognise an already stigmatised identity.

Based on this, the studies in the current chapter test whether those belonging to stigmatised groups may perceive greater group-based recognition

when surveillance is believed to be accurate (vs. less accurate). We also expect that greater perceptions of group-based recognition will predict more positive (and less negative) feelings towards surveillance (positive pathway). Conversely, we also expect more accurate surveillance to increase privacy concerns, which may in turn predict more negative (and less positive) feelings towards surveillance (negative pathway).

In Study 3a we examine stigmatised identity in the context of sexual orientation. Those identifying as gay have historically experienced discrimination and persecution (Jukes, 2016). Despite civil rights advances, today those identifying as gay continue to experience discrimination socially, medically, and economically (Emlet, 2016). To test our model in this context, Study 3a deviated from those in Chapters 2 and 3, as surveillance accuracy perceptions were measured rather than manipulated. The second study in this chapter tested our model within the context of veganism: an identity that challenges the political and cultural status quo. As such, the increasing popularity and visibility of the vegan identity has brought with it an associated stigma and backlash (Cole, 2011). Indeed, vegans report hostility, rejection, and conflict within their professional and social relationships after becoming vegan (Hirschler, 2011). In our second study we manipulated surveillance accuracy perceptions directly. Participants were provided with an article ostensibly from the Vegan Society, which described surveillance as having either low, medium, or high accuracy.

STUDY 3A

Method

Participants and design

Participants were recruited through the online platform Prolific Academic. In total, 386 responses were recorded; however, four participants withdrew before reading the description of algorithmic surveillance, and 12 participants completed none of the measures. This left 369 participants for data analysis. Of these, 55% were men (42% women; 2% non-binary; 1% preferred not to answer) and the majority identified as White (82%; 7% mixed race; 5% Asian; 4% Black, >1% Arab). Participants had a mean age of 31.44 years (*SD* = 11.33).[23]

The study was a cross-sectional survey. The predictor variable was perceptions of surveillance accuracy and the dependent variables were feelings towards surveillance. Potential mediators included perceived group-based recognition (distinctiveness, positivity, understanding, identification as a group member) and privacy concern.

Measures

Unless otherwise stated, responses were recorded on 7-point scales (1 = *Strongly disagree* to 7 = *Strongly agree*) and all negatively-phrased items were reverse scored. All measures may be found in Appendix K.

Identification. Four items were adapted from Doosje at al.'s (1995) identification scale to measure identification as gay. These items included 'I see myself as gay' and 'I am glad to be gay'. Scores on all items were averaged to create the final scale (α = .82, *M* = 5.49; *SD* = 1.18).

[23] The age data of two participants were deleted, as they answered with their year of birth rather than their age.

Perceived accuracy of surveillance. Four items measured how accurate participants believed algorithmic surveillance to be. Items included: 'In my view, algorithmic surveillance is accurate at identifying people' and 'in my view, algorithmic surveillance does not provide an accurate impression of internet users' (α = .88, *M* = 3.82; *SD* = 1.24).

Group-based recognition. The recognition measure was comprised of four sub-dimensions: distinctiveness, understanding, positivity, and identification as a group member. Identification as a group member was introduced in this study an additional recognition dimension. The measures referred to the extent to which participants felt that surveillance identified them as gay. A four-factor structure was supported by Confirmatory Factor Analysis (Appendix M).

Distinctiveness. This dimension measured the extent to which participants felt that their group was perceived as distinct. The measure included four items, such as 'algorithmic surveillance enables society to recognise that gay people are a unique group' and 'from algorithmic surveillance, society recognises that gay people have distinct needs' (α = .43, *M* = 3.62; *SD* = 0.91[24]).

Understanding. Four items assessed the degree to which participants felt that surveillance enabled their group to be understood. These items included 'algorithmic surveillance helps society appreciate gay people's values' and 'algorithmic surveillance provides society with a good understanding of what gay people believe' (α = .81, *M* = 2.95; *SD* = 1.04).

Positivity. Four items measured the extent to which participants felt their group was perceived positively. Items included 'Algorithmic surveillance helps promote the positive impact of gay culture within society' and 'gay people are

[24] Whilst reliability for this scale was low, we retained all items to preserve the a priori scale structure.

valued positively through algorithmic surveillance (α = .82, *M* = 3.57; *SD* = 0.98).

Identification as a group member. The degree to which participants felt surveillance identified them as gay was measured with two items: 'Through algorithmic surveillance, I believe I am identified as a gay individual' and 'Algorithmic surveillance does not identify me as gay' (*r* = .74; *M* = 4.44; *SD* = 1.54).

Privacy concern. Four items measured the extent to which surveillance made participants concerned for their privacy. These included 'surveillance online is an invasion of privacy' and 'people have a right to use the internet without being surveilled' (α = .76, *M* = 5.25; *SD* = 1.29).

Feelings towards surveillance. Identical to studies 2b and 2c, feelings towards surveillance were measured with two scales assessing positive emotion and negative emotion. Participants were asked, 'Algorithmic surveillance makes me feel…' and were then presented with 14 emotion items (seven items per scale).

Positive feelings*.* Scores on seven items, such as 'happy' and 'pleased', were averaged to form the positive feelings scale (α = .94, *M* = 2.75; *SD* = 1.18).

Negative feelings. Scores on seven items, such as 'angry' and 'anxious' were averaged to create the negative feelings scale (α = .90, *M* = 4.57; *SD* = 1.22).

Demographics. Participants were asked to indicate their age, gender, and nationality. Participants were also asked if they were openly gay; if they selected 'yes' or 'to some people, but not others', they were asked how many years and months they had been open about their sexuality.

Procedure

Participants were recruited via Prolific Academic. The site's screening tool was used to ensure that the study was only advertised to those who identified as gay. Once the survey was opened, participants were presented with a consent form that described the broad aims of the study. It also reiterated that the study was for those who identified as gay only. Once consent was given, participants were asked to write three things that were believed to be important to their sexuality, based on the method used by Haslam et al. (1999). This measure was included to increase the salience of participant's sexuality and was not analysed. Participants then completed the identification scale, before being presented with a brief description of algorithmic surveillance (Appendix L). The description outlined the various sources of surveillance (both private and state) and how information is shared between platforms. The social consequences of surveillance were also outlined, such as identifying people as security risks and what products and services people may be offered compared to others.

Once participants acknowledged that they had read the article (by clicking 'I have read the information above and wish to continue') they were presented with the remaining measures. Participants were given the opportunity to withdraw from the study on each page of the survey with a 'withdraw' button. On completion or withdrawal, participants were taken to a debrief page, which outlined the aims of the study in detail. At this point, they were also provided with links to websites that advise on personal data and privacy protection online, should they have felt concerned following the study. All participants were financially compensated at an hourly rate of £9.34.

Results

Missing data treatment

Missing data analysis revealed 0.04% of values were missing across all measures.[25] The expectation maximisation (EM) method was used in SPSS to impute the missing values, of which all fell within the scale range.

Structural models: Predicting feelings towards surveillance

A path analysis with manifest variables only was performed using the AMOS v24 package along with bootstrapping with 5000 samples and a 95% confidence interval. Correlations between variables can be found in Table 11.

Table 11. Summary of Pearson correlations between variables in the predicted model.

Measure	1.	2.	3.	4.	5.	6.	7.
1. Accuracy	-						
2. Distinctiveness	.45***	-					
3. Positivity	.36***	.42***	-				
4. Understanding	.39***	.53***	.70***	-			
5. Group identification	.27***	.18***	.15**	.17***	-		
6. Privacy concern	-.21***	-.26***	-.36***	-.38***	-.08	-	
7. Positive feelings	.10*	.23***	.45***	.49***	>.01	-.48***	-
8. Negative feelings	-.07	-.14**	-.36***	-.33***	-.03	.51***	-.63***

Note: * $p < .05$, ** $p < .01$, *** $p < .001$.

[25] This did not include the measures that asked participants to estimate the months/years they had been openly gay, as there were 64 missing cases for these measures. Additionally, participants had commented that this was too difficult to estimate so either guessed or skipped the measures entirely. Consequently, these measures were excluded from analyses.

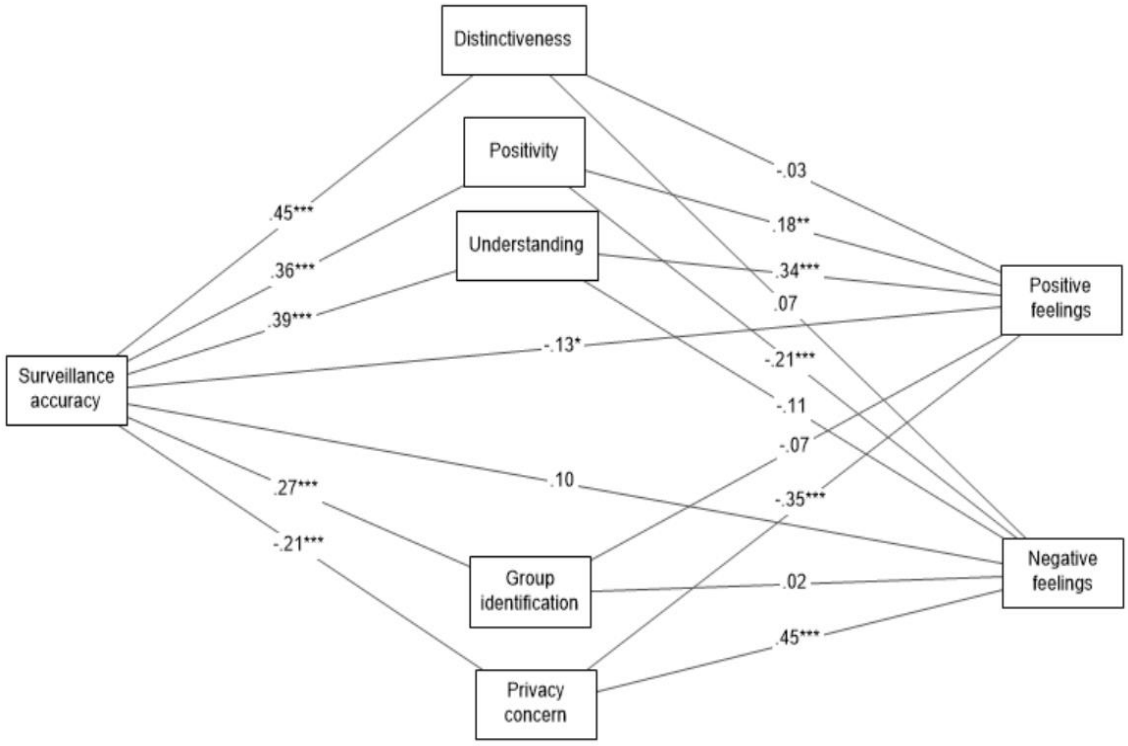


Figure 12. Path model illustrating the predicted model. Rectangles represent observed scale variables. Standardised coefficients for each relationship are depicted above path arrows along with significance values. Group-based recognition dimensions were covaried, as were positive and negative feelings towards surveillance. *Note:* * $p < .05$, ** $p < .01$, *** $p < .001$.

The predicted model demonstrated an adequate fit to the data, $\chi^2_4 = 51.06$, $p < .001$, $\chi^2/df = 12.77$, TLI = .649, CFI = .950, RMSEA = .179, AIC = 115.06.[26] Although the predicted model demonstrated an adequate at best fit, the primary aim of the analysis was to test countervailing paths rather than an overall model against a null.

[26] Whilst the chi-square test and its associated p-value is significant (suggesting poor fit) it is well documented that this test is sensitive to sample size, thus larger samples can often produce a statistically significant chi-square value (Vandenberg, 2006).

Effect of surveillance accuracy on group-based recognition and privacy concerns. The effect of accuracy was positive and significant for all group-based recognition dimensions. Perceiving surveillance as more accurate was associated with greater perceptions of distinctiveness (β = .45, $p < .001$), positivity (β = .36, $p < .001$), understanding (β = .39, $p < .001$), and being perceived as a group member (β = .27, $p < .001$).

Accuracy also had a significant effect on privacy concern: perceiving surveillance as more accurate was associated with *less* privacy concern, β = -.21, $p < .001$. This was in the opposite direction to what we expected, as we predicted that perceiving surveillance as more accurate would be associated with greater privacy concerns.

Effect of surveillance accuracy on feelings towards surveillance. Within the model, the direct effect of surveillance accuracy on positive feelings towards surveillance was significant, β = -.13, $p = .023$. More accurate surveillance was associated with less positive feelings towards surveillance. The direct effect of surveillance accuracy on negative feelings towards surveillance was marginally significant, β = .10, $p = .057$, in that more accurate surveillance predicted marginally more negative feelings towards surveillance.

Indirect effects. To examine the indirect effect for each potential mediator, the regression weights of all pathways between the independent variable and mediators were set to 0, aside from the mediator being examined. Summaries of indirect effects for positive and negative feelings towards surveillance are presented in Tables 12 and 13 respectively.

Positive feelings. There was a significant indirect path between surveillance accuracy and positive feelings towards surveillance through privacy

concern. Contrary to our expectations, surveillance of higher accuracy predicted *less* privacy concern. This in turn predicted more positive feelings towards surveillance. A marginally-significant indirect path was found through perceived positivity; perceiving surveillance as more accurate predicted more perceived positivity which in turn predicted more positive feelings towards surveillance. The indirect pathway of understanding and group identification approached significance and no indirect pathway was found through perceived distinctiveness.

Negative feelings. A significant indirect pathway was found between surveillance accuracy and negative feelings towards surveillance through privacy concern; less privacy concern predicted less negative feelings towards surveillance. A marginally-significant indirect pathway was found through perceived positivity: greater perceptions of positivity predicted less negative feelings towards surveillance. The indirect pathways through understanding, distinctiveness, and group identification were non-significant.

Table 12. Summary of indirect effects for positive feelings through each mediator variable in the predicted model.

Measure	β	*p*	95% CI (lower bound)	95% CI (upper bound)
Distinctiveness	-.01	.575	-0.04	0.02
Positivity	.01	.057	0.00	0.04
Understanding	.02	.090	-0.00	0.06
Group identification	-.02	.076	-0.04	0.00
Privacy concern	.07	.001	0.04	0.12

Table 13. Summary of indirect effects for negative feelings through each mediator variable in the predicted model.

Measure	β	*p*	95% CI (lower bound)	95% CI (upper bound)
Distinctiveness	.02	.180	-0.01	0.05
Positivity	-.02	.056	-0.05	0.00
Understanding	-.01	.111	-0.03	0.00
Group identification	.003	.674	-0.02	0.03
Privacy concern	-.09	.001	-0.15	-0.04

Discussion

The present study tested positive and negative pathways from perceived algorithmic surveillance accuracy to feelings towards surveillance amongst stigmatised group members. For the positive pathway, we tested whether perceiving surveillance as more accurate predicts greater group-based recognition, which in turn predicts more positive and less negative feelings towards surveillance. For the negative pathway, we tested whether perceiving surveillance as more accurate is associated with more privacy concern, which in turn predicts more negative and less positive feelings towards surveillance. The findings support the majority of these predictions.

The positive pathway

Surveillance accuracy perceptions are associated with group-based recognition. Perceptions of surveillance accuracy predicted all group-based recognition dimensions. Individuals felt greater group-based recognition when surveillance was perceived as more accurate. This tallies with previous social-veillance literature, which finds that individuals use digital platforms to curate their own identity and achieve recognition by either dispelling misconceptions or exaggerating desirable characteristics (Marwick, 2012; Steeves & Bailey, 2016). Our findings also go beyond this by demonstrating that recognition benefits can be experienced for group identities, as well as individual identities. It also supports the argument that individuals do not create a disconnect between their offline and online selves. As argued by Kennedy (2006), our identities online typically mirror those we embody in our offline lives. Therefore, groups that struggle for recognition in offline contexts may experience similar group-based recognition concerns when online. As discussed, stigmatised groups often seek opportunities to cultivate recognition during social interactions (Chrobot-Mason

et al., 2001; Miller & Kaiser, 2001). The present study provides cross-sectional evidence that accurate surveillance may satisfy the need for group-based recognition in an online context.

Group based recognition is associated with feelings towards surveillance. ***Positive feelings.*** Positivity and felt understanding were both associated with more positive feelings towards surveillance. However, it is worth noting that none of the group-based recognition dimensions have a strong *unique* predictive role in the model. When included together in the model the recognition dimensions appear to weaken or cancel out the effect of one another. Despite this, each dimension has a significant zero-order correlation with positive feelings towards surveillance, which suggests that the group-based recognition measure as a whole is more strongly associated with feelings towards surveillance rather than one specific dimension. As such, the following discussion relates to group-based recognition as a whole, rather than the individual dimensions.

Those that felt more group-based recognition were more likely to report positive feelings towards surveillance. Therefore, those that perceive surveillance as more accurate are more likely to feel group-based recognition, and in turn, more positive feelings towards surveillance. This supports research in marketing, which finds that people typically prefer online advertising that relates to their identity, attitudes, and interests (Campbell & Wright, 2008; McDonald & Cranor, 2010; Ur et al., 2012). Our findings extend this by highlighting the role of group identities in this process, suggesting that accurate surveillance has an intrinsic value through offering group-based recognition beyond the potential utility of relevant advertising (e.g. better product suggestions and discounts).

Whilst we have highlighted that each recognition dimension may have weakened the effect of the other dimensions in the model, it is worth exploring another possible reason as to why distinctiveness did not predict positive feelings towards surveillance. It could be argued that those identifying as gay may not want to be perceived as distinct. For example, the gay pride and LGBTQ+ movement have often coined the phrase ‘love is love’ to draw attention to the similarity between heterosexual and non-heterosexual relationships (Frumin, 2013). As such, group distinctiveness may not be a central component of the gay identity; therefore, participants may have felt ambivalent towards being perceived as distinct in this context.

Negative feelings. Positivity was the only recognition dimension to be uniquely associated with negative feelings towards surveillance, despite each dimension having a significant zero-order correlation with feelings towards surveillance: greater group-based recognition predicted less negative feelings towards surveillance in each case. Yet, when included together in the model each dimension weakened the effect of the others. As such, the group-based recognition measure as a whole may consistently predict feelings towards surveillance in a way that is not attributable to one particular dimension.

Whilst this may be the most likely explanation based on the findings, it could be suggested that although group-based recognition can encourage more positive feelings towards surveillance, recognition is not sufficient to undermine negative feelings. Indeed, a subset of literature has highlighted how those under surveillance often feel ambivalence towards surveilling systems. Typically, individuals report ambivalence from a heightened sense of security from surveillance yet a simultaneous invasion of privacy. For example, Ellis et al. (2013) found that participants felt surveillance was necessary to protect them

from crime (specifically terrorism), yet they also reported that surveillance felt like ‘Big Brother’ (p. 721). Our findings also indicate ambivalence, in that group-based recognition predicted positive feelings towards surveillance, yet this may not be sufficient to undermine negative feelings from privacy concern.

The negative pathway

Surveillance accuracy perceptions are associated with privacy concern. Those who perceived surveillance as more accurate reported *less* privacy concern than those who perceived surveillance as less accurate. This was contrary to our predictions and the findings from Study 1, whereby more accurate surveillance was associated with more privacy concern. It may be that surveillance of higher accuracy is simply more concerning when it relates to personal/individual identity (as demonstrated in Study 1) than when it pertains to the group. Results from Chapter 3 found no association between surveillance accuracy and privacy concern in Studies 2a and 2c, and found that perceiving surveillance as more accurate predicted *less* privacy concern in Study 2b. This suggests that in surveillance contexts, group privacy may be less concerning than individual privacy. Indeed, individuals typically report feeling safer in groups or crowds (Kern, 2005) and research has demonstrated that individuals are objectively safer in numbers (Jacobsen, 2015). Thus, it is possible that those under accurate surveillance feel better protected by the group from any consequences of surveillance accurate and therefore feel less concerned.

Privacy concern is associated with feelings towards surveillance. As expected, increased privacy concern was associated with more negative and less positive feelings towards surveillance. This is a key contribution to surveillance literature, as most research in this field includes privacy concern as

a dependent variable from which feelings or attitudes towards surveillance are inferred but rarely tested (e.g. O'Donnell et al., 2010a) or behavioural outcomes are assessed without the appraisals and affect that shape them (e.g., privacy paradox literature). Whilst perhaps intuitive, this research addresses this gap in the literature and demonstrates that when individuals feel an invasion of privacy they are more likely to feel negatively (and less positively) towards those surveillance systems.

Summary

The aim of the current study was to investigate whether members of a stigmatised group would appraise surveillance as a vehicle for group-based recognition when it was perceived as accurate. In turn, we expected these participants to feel more positively towards surveillance. On the other hand, we also expected stigmatised individuals to feel more *negatively* towards surveillance of greater accuracy, due to privacy concerns. The study provides support for the positive pathway through recognition, and suggests that the group-based recognition construct as a whole may have more predictive power than individual dimensions of recognition.

We also we found partial support for the negative pathway: privacy concern was associated with feelings towards surveillance. Contrary to our predictions, though, more accurate surveillance was associated with *less* privacy concern. Future research should explore whether privacy concern differs (i.e., is less concerning) when accurate surveillance is ostensibly focussed on the group compared to the individual. Additionally, it would be worth exploring whether conceptions of privacy and recognition differ across different social groups. Study 3b aims to address the latter point by testing the

predicted model within a vegan sample. We also manipulated surveillance accuracy directly.

STUDY 3B

In this second study, we focus on veganism, which is an identity with a less toxic history of discrimination and prejudice than is associated with sexual orientation, but with a current and contemporary sense of being stigmatised for a lifestyle choice.

Historically, vegans have experienced different social pressures than those identifying as gay. Vegans typically strive for outgroup equal treatment (non-human animals), whereas LGBT+ movements strive for ingroup equal treatment (e.g., those identifying as gay). Furthermore, those identifying as gay are often at greater risk of physical violence and danger from others (Hunter, 1990), whereas vegans have not historically faced the same intergroup threat. Nevertheless, vegans are also subject to misrecognition: they are commonly stereotyped as preachy (Linquist, 2013), hyper-feminine (Rothgerber, 2012) and are perceived more negatively than asexuals, homosexuals, immigrants, and atheists (MacInnis & Hodson, 2015).

In line with the studies reported in Chapters 2 and 3, the study employed an experimental design, whereby surveillance accuracy was manipulated to have three levels: low, medium, and high. Three treatment levels were chosen so that both linear and non-linear effects could be examined.[27] Our predictions remain the same as for Study 3a. We predicted that participants would report more recognition and privacy concerns when surveillance is described as

[27] For example, prior research suggests that individuals may feel more privacy concern as surveillance accuracy increases (Oulasvirta et al., 2012), whereas others suggest that concern may peak at low and high levels of surveillance accuracy (Ur et al., 2012). Three treatment levels enable us to explore both these possibilities.

having higher accuracy (vs. medium or low accuracy). In turn, we predicted that higher levels of group-based recognition would in turn predict more positive and less negative feelings towards surveillance. On the other hand, we expected higher levels of privacy concern to be associated with more negative and less positive feelings towards surveillance.

Method

Participants and design

Through purposive sampling, data were collected from 781 vegan individuals belonging to vegan Facebook groups online. Three hundred and seventy-one responses were deleted, as they had at least one measure with 100% missing data. This left 410 participants for the main analyses. The majority of participants were women (77%), while 20% were men, 3% identified as non-binary, and 1% preferred not to indicate their gender. Participants' mean age was 32.27 years (*SD* = 12.17) and most participants identified as White (91%; 3% mixed ethnicity, 3% Asian, 2% other, and < 1% Black or Arab). A sensitivity analysis using g*power indicated that the sample is sufficient to detect an effect using regression (four predictors), of $f = 0.14$ (partial $r = .14$) with 80% power for each of the effects of surveillance accuracy, distinctiveness, positivity, and privacy concern. The sample of the current study is also sufficient to detect an effect size using ANOVA of $f = 0.15$ ($\eta_p^2 = .02$) with 80% power for the main effect of surveillance accuracy ($df_{num} = 2$).

The study had a one-way between-participants experimental design. Accuracy was manipulated to have three levels: low, medium, and high. Participants were randomly allocated to one of these three conditions. Feelings towards surveillance (positive and negative) were included as the dependent

variable. Perceived group-based recognition (distinctiveness and positivity[28]) and privacy concern were measured as mediators. The study included additional measures that were not included in the final analysis.[29]

Measures

Unless otherwise stated, response scales used a 7-point format (1 = *Strongly disagree* to 7 = *Strongly agree*) and responses on all negatively-phrased items were reverse scored.

Manipulation. Participants were first asked to read an article ostensibly from the Vegan Society titled 'Being vegan online' (Appendix N). There were three versions of the article, which varied in how accurate they reported algorithmic surveillance to be. In the high accuracy condition, the article explained that products of online surveillance (targeted advertising) often suggested identity-relevant content (e.g., vegan cookbooks). In the low accuracy condition, the article argued that products of online surveillance rarely suggested identity-relevant content, and mostly provided non-vegan-related suggestions relating to dietary intolerance (e.g., gluten-free breaded meat). The medium accuracy condition reported that suggested material online was sometimes accurate but also sometimes inaccurate.

To reinforce the accuracy manipulation, participants were then presented with two fabricated screenshots of a Facebook news feed, which were described as being provided by vegan internet users. The screenshots depicted a large central suggested page/product and a smaller sidebar advert. In the high accuracy condition, both adverts were vegan related. In the low accuracy

[28] Following CFA (Appendix P), a two-dimension structure of recognition was considered superior to a three-factor solution in this study. Therefore, the distinctiveness dimension also includes the items from the understanding measure.

[29] Additional measures included: levels of identification, perceived motivation of surveiller, chilling effects, time spent online, and pre-manipulation measures of perceived recognition. All measures may be found in Appendix O.

condition both adverts were orientated towards a non-vegan restrictive diet (e.g., gluten-free). In the medium condition, one advert was related to veganism, whereas the other was associated with the non-vegan diet (location of the accurate/inaccurate adverts were counterbalanced).

Dependent measures. ***Manipulation check.*** Two items assessed whether participants understood the content of the article, and their perceptions of surveillance accuracy. Firstly, understanding of the article's content was measured with the item 'The Vegan Society article suggests that algorithmic surveillance is…', on a 7-point scale (1 = *Not at all accurate* to 7 = *Extremely accurate).* The second item related to participants' perception of surveillance accuracy: 'After reading the article, in my opinion algorithmic surveillance is…', answered on a 7-point scale (1 = *Not at all accurate* to 7 = *Extremely accurate).* The two items were averaged to create the final scale (r = .67, M = 3.77; SD = 1.29).

Group-based recognition. Recognition from algorithmic surveillance was then assessed. Despite theorising three separate group-based recognition dimensions (positivity, distinctiveness, understanding), distinctiveness and understanding items loaded onto the same factor. Therefore, the items from both these scales were combined. This produced two recognition dimensions for subsequent analyses: perceived intergroup distinctiveness and perceived positive group identity.

Distinctiveness. Intergroup distinctiveness was measured with eight items, such as 'Targeted adverts and webpage suggestions imply that my diet is the same as 'clean eating', 'Algorithmic surveillance enables omnivores to recognise that my beliefs towards food are distinct from those following other diets' and 'Algorithmic surveillance could help omnivores appreciate vegan

cultural values'. All items were included in the final scale (α = .77, *M* = 3.34; *SD* = .87).

Positivity. Perceived positive group identity measured how positively participants felt their group was viewed by other groups. This was measured with two items, including 'The results of algorithmic surveillance offer a positive image of veganism'. Both items were averaged to create the final scale (*r* = .58, *M* = 4.04; *SD* = 1.11).

Feelings towards surveillance. Identical to studies 2b, 2c and 3a, feelings towards surveillance was measured on two scales assessing positive emotion and negative emotion respectively. Participants were asked, 'Algorithmic surveillance makes me feel…' and were then presented with 14 emotion items (seven items per scale). Responses on all seven positive emotion items, such as 'happy', 'pleased', 'hopeful' and 'optimistic' were averaged to form the positive emotion scale (α = .93, *M* = 3.33; *SD* = 1.05), and responses on all seven negative emotion items, such as 'worried', 'annoyed', 'uncomfortable' and 'angry' were averaged to create the negative emotion scale (α = .90, *M* = 4.00; *SD* = 1.09).

Privacy concern. Privacy concerns were assessed using four items including 'Surveillance online is an invasion of privacy' and 'People's online data is not private information'. Scores were averaged to produce the final scale (α = .73, *M* = 4.90; *SD* = 1.21).

Demographics. Participants were asked to give their demographic information, including their age, gender, and ethnicity. Participants were also asked how many years and months they had been vegan.

Procedure

Participants were recruited via social media groups related to veganism. A link to the survey along with a brief description of the study was posted on each group. Once the link was opened, participants were asked to provide their consent before being randomly allocated to one of the three accuracy conditions. Once participants had read the article they were shown the two Facebook screenshots. After completing the remaining measures, participants were fully debriefed and provided with online sources concerning internet privacy.

Results

Missing data treatment

Analysis of missing data revealed that only 0.7% of values were missing across all measures. Missing values were imputed using the expectation-maximisation (EM) method in SPSS (Graham, 2009) and estimated values fell within the scale range.

Manipulation check

A one-way analysis of variance (ANOVA) revealed a significant effect of surveillance accuracy on the perceived accuracy of surveillance $F(2, 407) = 199.74$, $p < .001$, $\eta_p^2 = .495$. Pairwise comparisons revealed that those in the high accuracy condition ($M = 5.16$, $SD = 0.92$) reported higher accuracy perceptions than those in the medium accuracy condition ($M = 3.75$, $SD = 0.84$), $F(1, 407) = 154.90$, $p < .001$, $\eta_p^2 = .276$, 95% CI [1.19, 1.64]. Additionally, those in the medium accuracy condition reported greater accuracy perceptions than those in the low accuracy condition ($M = 2.60$, $SD = 1.05$), $F(1, 407) = 111.70$, $p < .001$, $\eta_p^2 = .215$, 95% CI [-1.36, -0.93]). Consequently, the manipulation was

considered successful. Correlations between all dependent measures may be found in Table 14.

Table 14. Summary of zero-order correlations between variables in the analyses.

Measure	1.	2.	3.	4.	5.
1. Accuracy perceptions	-				
2. Distinctiveness	.49***	-			
3. Positivity	.50***	.49***	-		
4. Privacy concern	-.09	-.08	-.01	-	
5. Positive emotion	.27***	.29***	.21***	-.31***	-
6. Negative emotion	-.24***	-.30**	-.27***	.33***	-.44***

Note: * $p < .05$, ** $p < .01$, *** $p < .001$.

Hypothesis testing: Mediation analysis

Mediation analysis was conducted using the SPSS PROCESS macro (Model 4; Hayes, 2013) to test the effect of surveillance accuracy on feelings towards surveillance (positive and negative) through group-based recognition (positivity and distinctiveness) and privacy concern. Sequential coding of the three-level accuracy manipulation was used, whereby surveillance accuracy was tested as two dummy variables: low versus medium and medium versus high.[30]

[30] Whilst this statistical technique does not allow the comparison of low and high accuracy, this comparison was not relevant to our predictions. We predicted linear findings, meaning a significant linear relationship between low versus medium and medium versus high intuitively demonstrates a linear relationship between low and high.

Positive emotion. ***Low versus medium accuracy.*** As shown in Figure 13, participants felt more recognised on both the positivity (*b* = .68, *p* < .001, *SE* = .12, 95% CI [0.45, 0.90]) and distinctiveness (*b* = .45, *p* < .001, *SE* = .09, 95% CI [0.27, 0.63]) dimensions when surveillance was described as being of medium accuracy compared to when it was described as low in accuracy. However, there was no effect of medium vs. low surveillance accuracy on privacy concern (*b* = .05, *p* = .710, *SE* = .14, 95% CI [-0.23, 0.34]). In turn, positive feelings towards surveillance were positively predicted by group distinctiveness (*b* = .25, *p* < .001, *SE* = .06, 95% CI [0.12, 0.38]), and negatively by privacy concerns (*b* = -.26, *p* < .001, *SE* = .04, 95% CI [-0.33, -0.18]). Believing that their group was perceived positively did not predict positive feelings toward surveillance (*b* = .08, *p* = .146, *SE* = .05, 95% CI [-0.02, 0.18]).

The indirect effect of surveillance accuracy through distinctiveness was significant, *b* = 0.11, *SE* = .04, 95% CI [0.04, 0.21], but was not significant through positivity, *b* = 0.05, *SE* = .04, 95% CI [-0.02, 0.14], or privacy concern *b* = -0.01, *SE* = .04, 95% CI [-0.09, 0.06]. The direct effect of surveillance accuracy on positive feelings towards surveillance was also significant: more positive feelings towards surveillance were reported when surveillance was described as being of medium accuracy compared to low accuracy, *b* = 0.26, *SE* = .12, *p* = .029, 95% CI [0.02, 0.49].

Medium versus high accuracy. Figure 13 illustrates that participants felt more recognition on both dimensions (positivity: *b* = .86, *p* < .001, *SE* = .12, 95% CI [0.62, 1.09]; distinctiveness: *b* = .58, *p* < .001, *SE* = .10, 95% CI [0.39, 0.77]) when surveillance was described as being of high accuracy compared to medium accuracy. Surveillance accuracy did not affect concern for privacy (*b* = -.10, *p* = .501, *SE* = .15, 95% CI [-0.40, 0.19]).

The indirect effect of surveillance accuracy on positive feelings towards surveillance was significant through perceived distinctiveness *b* = 0.15, *SE* = .05, 95% CI [0.05, 0.26], but not through positivity *b* = 0.06, *SE* = .05, 95% CI [-0.03, 0.04], or privacy concern *b* = 0.03, *SE* = .04, 95% CI [-0.04, 0.10]. The direct effect of surveillance accuracy was also not significant, *b* = -.09, *SE* = .13, *p* = .478, 95% CI [-0.34, 0.16].

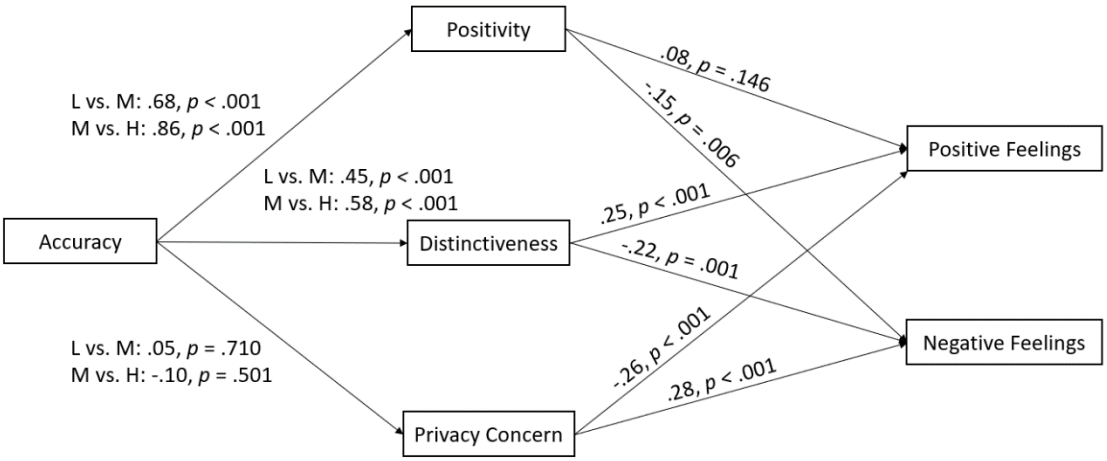


Figure 13. PROCESS path diagram for predicted model. Unstandardised regression coefficients and significance values are presented adjacent to each line that represents the relationship between variables.

Negative emotion. ***Low versus medium accuracy.*** As shown in Figure 13, perceived distinctiveness (*b* = -.22, *p* = .001, *SE* = .07, 95% CI [-0.35, -0.09]) and positivity (*b* = -.15, *p* = .006, *SE* = .05, 95% CI [-0.25, -0.04]) predicted less negative feelings towards surveillance. On the other hand, greater privacy concern predicted more negative feelings towards surveillance (*b* = .28, *p* < .001, *SE* = .04, 95% CI [0.20, 0.36]).

The indirect effects of surveillance accuracy on negative feelings towards surveillance through both positivity, *b* = -0.10, *SE* = .04, 95% CI [-0.20, -0.02] and distinctiveness, *b* = -0.10, *SE* = .04, 95% CI [-0.20, -0.03] were significant.

There was no significant indirect effect through privacy concern b = 0.02, SE = .04, 95% CI [-0.07, 0.10], and the direct effect of surveillance accuracy was also not significant, b = -0.10, SE = .12, p = .395, 95% CI [-0.34, 0.13].

Medium versus high accuracy. The indirect effect of surveillance accuracy was significant through positivity, b = -0.12, SE = .05, 95% CI [-0.23, -0.02] and distinctiveness, b = -0.13, SE = .06, 95% CI [-0.26, -0.03], but not through privacy concern b = -0.03, SE < .01, 95% CI [-0.11, 0.05]. There was also no direct effect of surveillance accuracy on negative feelings towards surveillance, b = -0.08, SE = .13, p = .520, 95% CI [-0.34, 0.17].

Discussion

Building upon Study 3a, the current study manipulated surveillance accuracy directly (low, medium, and high) and tested the predicted model in a different identity context (vegan identity) to ascertain whether our prior results are replicated within another stigmatised social group. Consistent with the previous studies in this thesis, the present study tested two opposing pathways that may explain feelings towards surveillance. A negative pathway was tested, whereby more accurate surveillance predicts more negative (and less positive) feelings towards surveillance through increased privacy concerns. A positive pathway was also tested: more accurate surveillance gives rise to greater feelings of group-based recognition, which in turn predicts more positive (and less negative) feelings towards surveillance.

Positive pathway: Accurate surveillance as a vehicle for group-based recognition

Overall, the majority of our predictions were supported. Recognition provided a positive pathway through which perceived accuracy of surveillance made members of a stigmatised group feel more favourably towards

surveillance. Specifically, surveillance accuracy indirectly predicted both positive and negative feelings towards surveillance through perceived distinctiveness. Additionally, an indirect path was also found through perceived positivity on negative feelings towards surveillance. Together, this suggests that when a group feels chronically misrecognised, members may receive recognition benefits through algorithmic surveillance when it is perceived as more accurate. In turn, group members are more likely to respond favourably towards those surveillance systems. These results highlight that despite the current negative rhetoric surrounding surveillance, positive psychological outcomes in the form of group-based recognition are possible when surveillance is perceived as accurate.

Negative pathway: Privacy concern

Contrary to expectations, we did not find an effect of surveillance accuracy on privacy concern: neither surveillance accuracy nor accuracy perceptions were associated with more privacy concern. However, higher privacy concerns did predict more negative and less positive feelings towards surveillance, as expected. The predicted negative pathway was therefore only partially supported.

It could be argued that for some groups, surveillance accuracy does not have a consistent effect on privacy concern over and above the presence of surveillance. For example, minorities such as Muslims often experience supra-visibility, whereby the mere presence of surveillance becomes a form of discrimination (Brighenti, 2007). Indeed, participants in Almuhumedi et al.'s (2015) study had concern over the fact that apps were accessing their data, rather than concern for any outcomes of gathering that data: '[I turned it off] because I can't think of a reason why Inkpad needs my location.' (p. 10); '…why

do you have to access my location thousands of times in [a] few days?' (p. 15). Whilst vegans have not historically been under social scrutiny, a surge in veganism over the last decade has prompted both the interrogation and criticism of the vegan movement (Cole & Morgan, 2011). Furthermore, animal rights activists continue to experience intense surveillance from government intelligence agencies (Boyer, 2017; Walby & Monaghan, 2011). For these groups, the issue of data access may be more of a concern than the subsequent accuracy of assumptions made from data collection. The same may not be said for those who do not experience supra-visibility.

As such, future research would benefit from testing both the positive and negative pathways in different group contexts. Whilst we theorised that recognition benefits from accurate surveillance would be more pronounced for those within chronically-misrecognised groups, it would be prudent to test this effect within groups who do not typically experience misrecognition. One possible outcome is that individuals may not experience any recognition benefits from surveillance, as their recognition needs have already been met – in other words, perceived surveillance accuracy will have little or no effect on perceived recognition. Indeed, this would tally with the findings from Study 2a, whereby surveillance accuracy perceptions predicted more group-based recognition when surveillance was conducted by the outgroup, but not the ingroup (as recognition needs are already met in this context).

Alternatively, inaccurate surveillance could raise *mis*recognition concerns in historically-recognised groups and function as a form of identity threat, meaning that the effect of surveillance accuracy on recognition will also be evident in less stigmatised groups. Future research could explore both these possibilities. Indeed, Study 2c explored the effects of surveillance accuracy

within a (typically non-stigmatised) British sample and found that inaccurate surveillance was indeed associated with misrecognition. Additionally, Study 4 of this thesis (reported in Chapter 5) directly manipulates group-based recognition to test whether accurate surveillance remedies a reduction in group-based recognition (and whether no recognition benefits are evident for those who already believed their group to be recognised).

GENERAL DISCUSSION

We argued in Chapter 2 that one reason why no association was found between surveillance accuracy and recognition in Study 1 is because recognition needs were not made salient. The aim of the studies in this chapter were to test the association between surveillance accuracy and recognition more precisely by making group-based recognition needs salient by recruiting those from stigmatised/chronically misrecognised groups and examining their feelings towards algorithmic surveillance at a group level. We expected that surveillance of greater accuracy would provide stigmatised individuals the opportunity for group-based recognition, and that this would in turn predict more positive (and less negative) feelings towards surveillance (positive pathway). Simultaneously, we also predicted that surveillance of greater accuracy would increase privacy concerns, and that this would produce countervailing effects on feelings towards surveillance (negative pathway).

Together, the two studies presented in this chapter provide varying levels of support for the positive and negative pathways in our predicted model. Surveillance accuracy (Study 3b) and surveillance accuracy perceptions (Studies 3a and 3b) were associated with greater perceived group-based recognition. In turn, more group-based recognition predicted more positive

feelings towards surveillance and (although less consistently) fewer negative feelings. For the negative pathway, Study 3a demonstrated an association between surveillance accuracy perceptions and privacy concerns, but this was in the opposite direction to what was expected; perceiving surveillance as more accurate predicted *fewer* privacy concerns. Additionally, Study 3b did not find an association between surveillance accuracy and privacy concern, which corroborates the findings from Chapter 3. However, both studies demonstrated that greater privacy concern does predict more negative and less positive feelings towards surveillance.

Positive pathway (1): Surveillance of greater accuracy is associated with more perceived group-based recognition

Both studies in this chapter provide evidence that stigmatised group members may perceive recognition benefits from accurate surveillance. Surveillance accuracy perceptions (Study 3a) and surveillance accuracy (Study 3b) predicted greater feelings of group-based recognition on all dimensions: distinctiveness, understanding, and positivity. As discussed, those belonging to stigmatised groups typically have a greater need for group-based recognition (Snow & Anderson, 1987) and will seek opportunities in which to increase recognition (Chrobot-Mason et al., 2001; Miller & Kaiser, 2001). Past research typically cites social interaction (often face-to-face) as an opportunity to bolster group-based recognition opportunities for these groups to achieve recognition (e.g., Newheiser & Barreto, 2014). The findings presented in this chapter suggest that accurate algorithmic surveillance may provide a further, unorthodox opportunity for stigmatised groups to achieve recognition benefits.

For example, the studies presented in this chapter suggest that recognition processes are also present in surveillance contexts which do not

involve friends and/or familiar others. Outside of peer groups and social networks, individuals may also receive benefits of recognition from corporate or government institutions. Recognition in these contexts is perhaps less expected, as these organisations are typically less trusted (Ellis et al., 2013).

It could also be argued that these contexts may provide a less pressured, potentially safer avenue for recognition than face-to-face interaction. For example, stigmatised individuals often conceal problematic identities in social contexts (Goffman, 1963; Newheiser & Barreto, 2014) or avoid social interactions and spaces from fear of harassment or even violence (Corteen, 2002). Whilst algorithmic surveillance can pose a threat to personal security and opportunity when mishandled (O'Neil, 2016), it arguably does not present the same immediate threat and anxiety that personal interaction may present for those that are stigmatised. As such, algorithmic surveillance may provide a safer avenue for stigmatised groups to enhance group-based recognition compared to traditional yet more dangerous face-to-face interaction.

In common with Studies 2a-2c, the studies in this chapter also illustrates the importance of social identity within surveillance contexts. Previous research has predominantly explored how individuals might achieve identity recognition online from platforms that emphasise individual rather than group-based characteristics. For example, prior work on participatory surveillance has found that surveillance from peers on social media, and subsequent accurate feedback, increases perceptions of interpersonal recognition (Albrechtslund, 2008; Steeves & Baily, 2016; Toma & Hancock, 2013). However, shared group characteristics are often unexplored within these contexts; individuals are thought to seek recognition for more personal experiences and attributes: 'like a

personal ad…I do, actually [think of my Facebook profile as a store about myself]' (Steeves & Baily, 2016, p. 8).

A small amount of prior research has acknowledged the concern for group-based recognition online. For instance, Stuart and Levine (2017) conducted focus group interviews exploring attitudes towards surveillance in which group identity concerns emerged. One participant spoke of having her gender on Facebook misrecognised as male and was in turn exposed to gay dating advertisements, which made her feel unfavourably towards the platform: 'But then I started getting adverts for gays all around [location]…and I was like no thanks I am really not interested in that…I was like ah!' (p. 701). This suggests that individuals are aware of the groups that they are assumed to belong to and appraise surveillance based on these assumptions. The studies in this chapter build on this by providing an experimental test of the group-based identity concerns that are present within surveillance contexts and how these concerns can shape how we feel towards surveillance systems online (discussed below).

Positive pathway (2): Greater perceptions of group-based recognition predict more positive and less negative feelings towards surveillance

In turn, those who perceived greater group-based recognition from algorithmic surveillance were generally more likely to feel positively (and less negatively) towards the surveillance system. However, there are some caveats. In Study 3a, positivity was the only recognition dimension to uniquely predict negative feelings towards surveillance. Group-based recognition more consistently predicted positive feelings towards surveillance. This mirrors the findings from Studies 2b and 2c, whereby none of the recognition dimensions uniquely predicted negative feelings towards surveillance. As discussed earlier

in this chapter, our findings suggest that each recognition dimension does not have a consistent, unique predictive role in our model; instead, group-based recognition *as a whole* is the basis for feelings towards surveillance.

Whilst less likely, we have also suggested that these findings suggest ambivalence towards surveillance, whereby increased group-based recognition may encourage people to feel more favourably towards surveillance, yet these identity benefits do not mitigate negative feelings towards surveillance. Indeed, ambivalence towards surveillance has been documented elsewhere. For example, in Ellis et al.'s (2013) research, participants reported some positive feelings towards surveillance, as they believed it to enhance public safety: 'I quite like them cause I feel safe' (p. 721). However, the same participant also described feeling negatively because of privacy infringements: 'I mean it is big daddy they know exactly really what you buy' (p. 721). Another participant also reported safety benefits but also felt conflicted: '…it's invasion I just don't like it…this is where I get conflicts you see' (p. 721). Koskela (2000) also highlights the public's ambivalence towards surveillance, as surveillance systems can inspire feelings of both safety and mistrust. Our findings support these positions, but also suggest that positive feelings may also arise from group-based recognition. Therefore, together with the literature cited above, it could be argued that ambivalence towards surveillance may be predicted by safety concerns, privacy concerns *and* perceived recognition.[31]

Distinctiveness did not uniquely predict positive or negative feelings towards surveillance in Study 3a. Distinctiveness refers to a central motive

[31] It is important to note that Study 3b demonstrated a relationship between group-based recognition and negative feelings towards surveillance. Nevertheless, as this finding is not consistent amongst our studies further research is necessary to establish the circumstances where group-based recognition has the potential to mitigate negativity towards surveillance.

described in SIT (Tajfel & Turner, 1979), whereby individuals strive for their group to be seen as positively distinct from others. The results presented in this chapter suggest that the degree to which individuals appraise surveillance based on recognition may depend on the group to which they belong. It could be argued that those identifying as gay do not prioritise distinctiveness. For example, the gay rights movement has historically fought for equal treatment and respect. It was only in 1973 that the American Psychiatric Association removed homosexuality from its list of mental illnesses (Kozuch, 2017) and gay marriage was only legalised in the UK in 2014 ('Gay Marriage Legalised at Midnight in England and Wales', 2014). Therefore, the gay rights movement has typically advocated the similarities between homosexual and heterosexual love, and as such argued that both deserve equal treatment. Consequently, gay individuals may not perceive *difference* to be an important facet of a gay identity, and may therefore be unlikely to feel differently towards algorithmic surveillance on the basis that it provides group-based distinctiveness.

The same may not be true for those identifying as vegan (Study 3b). The vegan movement typically strives for the vegan lifestyle to be considered positively, but also as distinct. For example, on the Vegan Society's website in a section titled 'Why go vegan?' the site lists benefits for animal welfare, the environment, and health as reasons why an individual might choose veganism. The group may also equally value distinctiveness. Veganism is typically confused with 'plant-based' (The Happy Pear, n.d.) and other restrictive diets such as those that eliminate lactose and gluten (Radical Preachy Vegan, 2015). This suggests that both distinctiveness and positivity may be central to the recognition needs raised by a vegan identity. As such, whilst distinctiveness did not play a (unique) role in predicting feelings towards surveillance in Study 3a,

this may not be the case for other social groups where distinctiveness is of higher importance to the self-concept. Consequently, future research should be mindful of the content of identity concerns when examining group-based recognition.

Negative pathway (1): Surveillance of greater accuracy is not associated with more privacy concern

The findings from this chapter mirror those from Chapter 3, in that surveillance accuracy was not consistently associated with privacy concern. In fact, whilst surveillance accuracy *perceptions* predicted privacy concern in Study 3a, this was in the opposite direction to what was expected; when surveillance was perceived as having greater accuracy participants reported *less* privacy concern. Additionally, the manipulation of surveillance accuracy and surveillance accuracy perceptions in Study 3b were not associated with reported privacy concern.

In Study 3a it could be argued that perceiving surveillance as highly accurate was associated with *fewer* privacy concerns because individuals perceive their privacy as a fair trade when accurate surveillance may benefit the group. This phenomenon was demonstrated by Pavone and Esposti (2010), who found that individuals either felt a surveilling institution enhanced their security without compromising their privacy or compromised their privacy without security benefits. Our findings may mirror those from Pavone and Esposti, as those who perceived surveillance as highly accurate perceived greater benefits from surveillance (in the form of group-based recognition) and fewer disadvantages (in the form of less privacy concern).

However, it is worth noting that a negative association between surveillance accuracy perceptions and privacy concern was only found in Study 3a (and Study 2b) and does not replicate the findings from Studies 1, 2a, 2c, or 3b. It is unclear why those identifying as gay may experience accurate surveillance as wholly advantageous, when other groups do not demonstrate the same reduction of privacy concern. As such, future research should endeavour to replicate these findings to establish whether this was anomalous or a unique phenomenon to those identifying as gay and this should in turn be unpacked.

Study 3b replicates the findings from Chapter 3, as no association was found between surveillance accuracy and privacy concern. The results also closely replicate those from Study 2c, as neither surveillance accuracy nor surveillance accuracy perceptions were associated with privacy concern. As discussed above, it is likely that the presence of surveillance per se (versus its absence) affects privacy concern separately from its accuracy. Therefore, it could be that vegan participants felt surveillance itself was a privacy infringement, irrespective of its accuracy. Indeed, the mean level of privacy concern across conditions was 4.90 (on a 7-point scale), which suggests that privacy concern was generally high for participants. Additionally, Sylvestre (2009) suggests an association between veganism and anti-establishment views; therefore, vegans in particular may express a greater opposition (and concern for privacy) towards governing institutions and surveillance systems generally.

Negative pathway (2): Greater privacy concern is associated with less positive and more negative feelings towards surveillance

Both studies in this chapter supported our predictions that greater privacy concern would be associated with less positive and more negative feelings towards surveillance. These findings mirror those from Chapter 3.

Little previous research has examined the relationship between privacy concern and feelings towards surveillance. Typically, negative (or less positive) feelings are assumed if an invasion of privacy has been experienced. Whilst this association is perhaps intuitive, little empirical research exists to support this association. Qualitative evidence has suggested a relationship between privacy concern and feelings towards surveillance. For example, in Stuart and Levine's (2017) study, one participant reported that surveillance from Google was 'really weird and I don't like them doing that' (p. 699) and another participant drew an association between privacy concerns and feelings towards surveillance in relation to Google Glass 'glasses that are recording everything…I don't really like it…a bit big brothery' (p. 700). This chapter substantiates this research by providing empirical evidence that greater privacy concern increases more negative and less positive feelings towards surveillance technologies.

These findings also speak to the complex relationship internet users have with surveillance systems. For example, in privacy paradox research, individuals who feel high levels of privacy concern may continue to engage with a surveilling site or do little to alter their online behaviour (see Gerber, Gerber, & Volkamer, 2018 for a review). Whilst we did not measure behavioural outcomes, our research suggests that individuals may continue interacting with a surveilling platform whilst experiencing privacy concern *and* feeling negatively towards the platform itself. This highlights the potential strength of positive

outcomes associated with these platforms (or negative outcomes associated with disengagement); despite privacy concern *and* a relative dislike for a platform, individuals may continue to engage with it.

Future research

Future research should endeavour to further examine the association between surveillance accuracy and privacy concern. Studies 2b and 3a suggests that for some groups, more accurate surveillance may indeed *reduce* privacy concerns, whereas Study 3b found no association between surveillance accuracy and privacy concern. In cases where no association is found, future research could examine whether the *presence* or *amount* of surveillance is a bigger driver of perceived invasion of privacy, over and above variation in the perceived accuracy of that surveillance.

Future research should also test the association between surveillance accuracy and privacy concern within social groups that differ in terms of social position, including different social status. As discussed, the effect of surveillance accuracy on privacy concerns may be stronger in groups who do not experience supra-visibility and persecution through surveillance. Members of groups that *do* have a negative history with surveillance and persecution through surveillance, such as groups that have been victimised by aggressive and/or chronic surveillance techniques, may be less sensitive to variations in surveillance accuracy. Therefore, by testing the model within different group contexts the boundaries of our current model may be clarified.

Thus far, we have argued that accurate surveillance may only provide recognition benefits when identity needs are made salient. To make identity needs salient, we employed intergroup contexts in Chapter 3, and recruited

those from stigmatised groups in Chapter 4. By doing this, both chapters provide converging evidence of the association between surveillance accuracy/surveillance accuracy perceptions and group-based recognition. The following chapter aims to directly test our assumption that the association between surveillance accuracy and recognition is due to a need for group-based recognition. We do so by manipulating group-based (mis)recognition directly within Welsh participants to test whether the effect of surveillance accuracy on group-based recognition is more pronounced when an ingroup is believed to be historically misrecognised (vs. recognised).

CHAPTER 5

STUDY 4

One limitation of the studies reported in Chapters 3 and 4 is that group-based (mis)recognition concerns were assumed (by making intergroup comparisons salient in Chapter 3; and sampling from stigmatised groups in Chapter 4), rather than directly manipulated. In light of this, the study reported in this chapter not only replicates the effect of surveillance accuracy on group-based recognition (and in turn the relationship between group-based recognition and feelings towards surveillance), but also orthogonally manipulates historical/chronic group-based (mis)recognition. This allowed us to test whether the effect of surveillance accuracy on group-based recognition evident in Chapter 4 was indeed stronger when individuals experience identity threat/misrecognition (an accuracy X chronic-misrecognition interaction), or whether the effect of accuracy is evident regardless of chronic-misrecognition (a main effect of accuracy, unmoderated by chronic-misrecognition).

The current study tests these possibilities by manipulating both chronic/historic (mis)recognition and surveillance accuracy. A Welsh demographic was chosen for the purposes of this study, as Wales and Welsh people experience both national celebration *and* prejudice. Welsh people and culture are currently and historically stigmatised in an English context (e.g., frequent negative portrayals by public figures and in the media; Cosslett, 2018). However, there are also countless examples of Welsh achievements that have also been recognised worldwide (e.g. Baroness Tanni Grey-Thompson's athletic achievements; Breen, 2018). As such, we drew upon examples of recognition of Welsh pride and achievement for the recognition condition, and

examples of disregard or misunderstanding of the Welsh for the misrecognition condition. A sample of people who identify as Welsh were presented with an article that either described Wales as being recognised and celebrated globally (recognition condition), or an article that described Wales as globally misrecognised and overlooked (misrecognition condition). The surveillance accuracy manipulation was then presented.

We aimed to test between two possible effects: a main effect of surveillance accuracy only, or an interactive effect between surveillance accuracy and (mis)recognition. For the former, we predicted that surveillance of greater accuracy would be associated with more perceived group-based recognition, irrespective of (mis)recognition condition. For the latter, we predicted that an association would be found between surveillance accuracy and group-based recognition *only* when they perceived their group to be chronically misrecognised (misrecognition condition). Conversely, we did not predict those in the recognition condition would perceive recognition benefits from accurate surveillance, as their recognition needs are ostensibly met.

Based on our overall model, we predicted that more accurate surveillance would lead to greater privacy concern (the negative pathway). In turn, we anticipated that greater privacy concern would predict more negative and less positive feelings towards surveillance. A main effect of (mis)recognition was not expected, nor do we expect an interaction. To our knowledge, there is no evidence (empirical nor theoretical) that would suggest (mis)recognition is conceptually related to privacy concern. As discussed throughout this thesis, stronger predictors of privacy concern are the presence (compared to absence) of surveillance and the presentation of surveillance (e.g. the source of

surveillance, its potential consequences, and its accuracy; please refer to Chapters 1 and 3 for an overview).

Method

Participants and design

Participants were recruited via Prolific Academic. A total of 417 participants took part in the study; however 23 cases were deleted, as at least one dependent measure scale was incomplete. Therefore, a total of 394 participants were included in the final sample. Of these, 68% were women (32% men) and one individual identified as non-binary. Participants' mean age was 36.46 years (*SD* = 13.13), and the majority of participants identified as White (95%; 2% mixed race, 2% Asian, >1% Black). A sensitivity analysis using g*power indicated that the sample of 394 is sufficient to detect an effect size using MANOVA of $f = 0.15$ ($\eta_p^2 = .02$) with 80% power for the main effects of and interaction between surveillance accuracy and (mis)recognition (two predictors; six groups). When using regression (four predictors), the current study is sufficient to detect an effect size of $f = 0.14$ (partial $r = .14$) with 80% power for each of the effects of distinctiveness, understanding, positivity, and privacy concern.

The study had a 2 (chronic (mis)recognition: recognised vs. misrecognised) X 3 (accuracy of surveillance: low, medium, and high) factorial between-participants design. Participants were randomly assigned to one of the six conditions (manipulation material may be found in Appendix Q). Dependent variables were feelings towards surveillance (positive and negative) and

potential mediators included recognition (positivity, distinctiveness, understanding) and privacy concern.[32]

Measures

Unless otherwise stated, responses were recorded on a 7-point scale (1 = *Strongly disagree* to 7 = *Strongly agree*). Negatively-phrased items were reverse coded.

Identity salience. Participants were asked to write three things that they felt made Welsh people different from those belonging to other nationalities (based on Haslam et al., 1999). This was included to ensure that the Welsh identity was salient at the time of completing the survey.

Identification. Four items were adapted from Doosje et al.'s (1995) identification scale to measure identification as Welsh. Items included 'I identify with other Welsh people' and 'I am glad to be Welsh'. All items were used for the final identification scale (α = .83, *M* = 5.44; *SD* = 0.84).

Recognition manipulation. Participants were shown an article extract ostensibly from a popular online news website. The extract was titled either: 'Wales – a celebrated nation' (recognition condition) or 'Wales – an invisible nation?' (misrecognition condition). The extract described Wales as being either recognised globally, or not. In the recognition condition, examples of St David's Day (the patron saint day of Wales; a national day of celebration) 'Google Doodles'[33] were included to reinforce the manipulation. For the misrecognition

[32] Other measures were included in the survey but were not part of the analyses. All measures may be found in Appendix R.
[33] Google Doodles are variations in how the Google logo is portrayed on the Google home page. The logo is often artistically reimagined to reflect significant historic anniversaries or dates.

condition, a picture of the UK with Wales missing was included to reinforce the manipulation (a genuine image from a European Union reference book[34]).

Recognition manipulation check. Seven items were included to check the effectiveness of the recognition manipulation. Five items were positively worded items adapted from the recognition measure (below).[35] One item was included to check that participants understood the content of the article: 'the article suggests that Welsh people are well recognised by wider society'. An additional item measured perceived discrimination: 'Welsh people are mistreated by wider society'. All seven items were included to form the final scale (α = .88, *M* = 4.06; *SD* = 1.40).

Accuracy manipulation. Participants were shown a second, ostensibly genuine article extract supposedly from the same news website. The article first described algorithmic surveillance before explaining that 89% of Welsh people found it accurate (high accuracy condition), 50% found it accurate (medium accuracy condition), or 89% of Welsh people found it inaccurate (low accuracy condition). Specifically, the article stated that Welsh people were rarely/sometimes/frequently miscategorised as English and provided English content. To reinforce the manipulation, examples of targeted Facebook material were shown (high accuracy: four adverts containing Welsh content; medium accuracy: two adverts containing Welsh content, two adverts containing English content; low accuracy: four adverts containing English content).

Accuracy manipulation check. Five items were included to assess the effectiveness of the accuracy manipulation (e.g., 'In my view, algorithmic

[34] BBC (2004).
[35] The recognition manipulation referred to how participants felt Wales and Welsh people were recognised generally (independent of surveillance). This differed from the main recognition measure, which related to (mis)recognition *as a result of* algorithmic surveillance.

surveillance creates an accurate impression of internet users'). Scores on the five items were averaged to create the final scale (α = .88, *M* = 3.57; *SD* = 1.33).

Perceived group-based recognition. Recognition was divided into three dimensions: positivity, distinctiveness, and understanding. Confirmatory Factor Analysis supported a three-factor structure (Appendix S).

Positivity. Four items measured how positively participants felt Welsh people were perceived by others (e.g. 'Welsh people are valued positively through algorithmic surveillance'). All four items were averaged to create the final scale (α = .88, *M* = 4.00; *SD* = 1.14).

Distinctiveness. Four items measured the extent to which participants felt surveillance recognised Welsh people as a distinct nationality. Items included 'Algorithmic surveillance enables society to recognise that Welsh people are a unique nationality'. Scores on all four items were averaged to create the final scale (α = .73, *M* = 3.55; *SD* = 1.23).

Understanding. Four items measured the extent to which participants felt surveillance led to good understanding of the Welsh identity, such as 'Algorithmic surveillance helps wider society appreciate Welsh people's values'. All four items were used to create the final scale (α = .88, *M* = 3.35; *SD* = 1.22).

Feelings towards surveillance. Identical to our previous studies, feelings towards surveillance were measured with two scales: positive emotion and negative emotion. Participants were asked, 'Algorithmic surveillance makes me feel…' and were then presented with fourteen emotion items (seven items per scale).

Positive feelings. All seven items, such as ‘happy’ and ‘pleased’ were averaged to form the positive feelings scale (α = .89, *M* = 4.96; *SD* = 1.00).

Negative feelings. All seven items, such as ‘angry’ and ‘anxious’ were averaged to create the negative feelings scale (α = .89, *M* = 2.91; *SD* = 1.20).

Privacy concern. Four items measured the extent to which participants felt surveillance compromised their privacy. Items included ‘Surveillance online is an invasion of privacy’ and ‘people have a right to use the internet without being surveilled’. All items were used to create the final scale (α = .63, *M* = 4.88; *SD* = 1.13).

Demographics. Participants were asked to provide their age, gender, and ethnicity. They were also asked how long they spent online, whether they belonged to closed/private groups online, and how aware they were of surveillance online (1 = *Not at all aware* to 10 = *Very aware*).

Procedure

Participants were recruited through Prolific Academic, an online research participation system. The site’s screening tool was used to ensure that the study was only made accessible to those who identified as Welsh. Participants were presented with a brief description of the study before continuing to the consent form. After giving their informed consent, participants completed the pre-manipulation measures before being randomly allocated to one of the six conditions. They were then shown the article relating to recognition of the Welsh identity before being asked to complete the recognition manipulation check measure. They were then presented with the article relating to surveillance accuracy, after which they were asked to complete the accuracy manipulation check and remaining dependent measures. On completion or withdrawal,

participants were fully debriefed and provided with online sources pertaining to internet privacy online should they feel concerned. Participants were financially compensated at a rate of £7.52 per hour.

Results

Missing data treatment

Analysis of missing data revealed that only 0.2% of values were missing across all measures. Missing values were imputed using the expectation-maximisation (EM) method in SPSS (Graham, 2009) and all estimated values fell within the scale range.

Manipulation checks

Accuracy. A two-way ANOVA was used to test whether the surveillance accuracy manipulation affected participants' perception of surveillance accuracy. A significant effect of surveillance accuracy was found on perceptions of surveillance accuracy, $F(2, 388) = 177.14$, $p < .001$, $\eta_p^2 = .477$. Those in the high accuracy condition ($M = 4.78$, $SD = 0.99$) perceived surveillance as more accurate than those in the medium accuracy condition ($M = 3.38$, $SD = 0.95$; $p < .001$). Additionally, those in the medium accuracy condition perceived surveillance as significantly more accurate than those in the low accuracy condition ($M = 2.57$, $SD = 0.95$; $p < .001$). Those in the high accuracy condition reported significantly higher accuracy perceptions than those in the low accuracy condition ($p < .001$). Therefore, the accuracy manipulation was considered successful. The (mis)recognition manipulation did not affect surveillance accuracy perceptions ($F(1, 388) = 0.16$, $p = .692$, $\eta_p^2 < .001$), and there was no evidence of an interaction between (mis)recognition and surveillance accuracy ($F(2, 388) = 1.32$, $p = .267$, $\eta_p^2 = .007$).

Recognition. A similar two-way ANOVA was used to test whether the (mis)recognition manipulation affected participants' feelings of group-based recognition. A significant effect of (mis)recognition was found for perceived recognition, $F(1, 388) = 514.09$, $p < .001$, $\eta_p^2 = .570$. Those in the misrecognised condition ($M = 3.01$, $SD = 0.92$) perceived significantly less recognition than those in the recognised condition ($M = 5.12$, $SD = 0.93$). Consequently, the recognition manipulation was considered successful. Surveillance accuracy was not associated with chronic group-based recognition ($F(2, 388) = 0.85$, $p = .427$, $\eta_p^2 = .004$), and there was no evidence of an interaction between surveillance accuracy and (mis)recognition ($F(2, 388) = 0.02$, $p = .984$, $\eta_p^2 < .001$). Table 15 presents the correlations between the measured (dependent) variables in the study.

Table 15. Summary of Pearson correlations between dependent variables in the predicted model.

Measure	1.	2.	3.	4.	5.	6.	7.
1. Accuracy check	-						
2. Recognition check	.13*	-					
3. Positivity	.69***	.30***	-				
4. Understanding	.65***	.26***	.73***	-			
5. Distinctiveness	.76***	.18***	.76***	.74***	-		
6. Privacy Concern	-.11*	-.01	-.14**	-.21***	-.14**	-	
7. Positive feelings	.13**	.15**	.17**	.13*	.12*	-.07	-
8. Negative feelings	-.10*	-.15**	-.13*	-.08	-.09	-.06	-.71***

Note: * $p < .05$, ** $p < .01$, *** $p < .001$.

Hypothesis testing

Feelings towards surveillance. A 2(chronic (mis)recognition: recognised, misrecognised) x 3 (surveillance accuracy: low, medium, and high) multivariate analysis of variance (MANOVA) was conducted with positive and negative feelings entered as dependent variables. The multivariate main effect of (mis)recognition was not significant, Wilks' Lambda = 1.00, $F = 0.75$, $p = .472$, $\eta_p^2 = .004$. The multivariate main effect of surveillance accuracy was not significant, Wilks' Lambda = 1.00, $F = 0.35$, $p = .847$, $\eta_p^2 = .002$. There was no evidence of a multivariate interaction between (mis)recognition and surveillance accuracy, Wilks' Lambda = 1.00, $F = 0.38$, $p = .825$, $\eta_p^2 = .002$.

Positive feelings. No main effects were found of surveillance accuracy, $F(2, 388) = 0.46$, $p = .635$, $\eta_p^2 = .002$, or chronic (mis)recognition, $F(1, 388) = 0.004$, $p = .949$, $\eta_p^2 < .001$, on positive feelings towards surveillance. Additionally, the interaction between surveillance accuracy and (mis)recognition on positive feelings towards surveillance was not significant, $F(2, 388) = 0.56$, $p = .576$, $\eta_p^2 = .003$.

Negative feelings. No main effect was found for surveillance accuracy on negative feelings towards surveillance, $F(2, 388) = 0.45$, $p = .638$, $\eta_p^2 = .002$, nor chronic (mis)recognition, $F(1, 388) = 0.83$, $p = .362$, $\eta_p^2 = .002$. No interaction was found between surveillance accuracy and (mis)recognition on negative feelings towards surveillance, $F(2, 388) = 0.31$, $p = .735$, $\eta_p^2 = .002$.

Positive psychological outcomes: Group-based recognition. A second 2(chronic (mis)recognition: recognised, misrecognised) X 3 (surveillance accuracy: low, medium, and high) MANOVA was conducted with distinctiveness, positivity, and understanding entered as dependent variables.

The multivariate main effect of (mis)recognition was significant, Wilks' Lambda = .96, $F = 5.55$, $p = .001$, $\eta_p^2 = .041$. A significant multivariate main effect was also found for surveillance accuracy, Wilks' Lambda = .55, $F = 45.37$, $p < .001$, $\eta_p^2 = .261$. There was no indication of a multivariate interaction between chronic (mis)recognition and surveillance accuracy, Wilks' Lambda = .98, $F = 1.40$, $p = .212$, $\eta_p^2 = .011$.

Distinctiveness. A significant main effect of surveillance accuracy was found on distinctiveness, $F(2, 388) = 135.28$, $p < .001$, $\eta_p^2 = .411$, with those in the low accuracy condition ($M = 2.70$, $SD = 0.92$) reporting significantly less distinctiveness than those in the medium accuracy condition ($M = 3.37$, $SD = 0.93$, $p < .001$). Additionally, those in the medium accuracy condition reported significantly less distinctiveness than those in the high accuracy condition ($M = 4.60$, $SD = 1.00$, $p < .001$). The high accuracy condition was also associated with significantly more distinctiveness than the low accuracy condition ($p < .001$).

There was no main effect of chronic (mis)recognition on perceived distinctiveness, $F(1, 388) = 0.002$, $p = .965$, $\eta_p^2 < .001$, and no interaction was found between surveillance accuracy and (mis)recognition, $F(2, 388) = 2.27$, $p = .105$, $\eta_p^2 = .012$.

Understanding. A significant main effect was found for surveillance accuracy on felt understanding, $F(2, 388) = 58.94$, $p < .001$, $\eta_p^2 = .233$. Those in the low accuracy condition ($M = 2.67$, $SD = 0.94$) reported significantly less understanding than those in the medium accuracy condition ($M = 3.31$, $SD = 1.10$, $p < .001$). Those in the medium accuracy condition reported significantly less understanding than those in the high accuracy condition ($M = 4.09$, $SD = 1.17$, $p < .001$). Highly accurate surveillance was also associated with

significantly more felt understanding than surveillance of low accuracy (p < .001).

No main effect was found for chronic (mis)recognition on felt understanding, $F(1, 388) = 0.36$, $p = .551$, $\eta_p^2 = .001$. The interaction between (mis)recognition and surveillance accuracy approached significance, $F(2, 388) = 2.72$, $p = .067$, $\eta_p^2 = .014$, however the effect of accuracy was significant for both the recognition, $F(2, 388) = 23.03$, $p < .001$, $\eta_p^2 = .106$ and misrecognition groups , $F(2, 388) = 38.17$, $p < .001$, $\eta_p^2 = .164$ (see Figure 14).

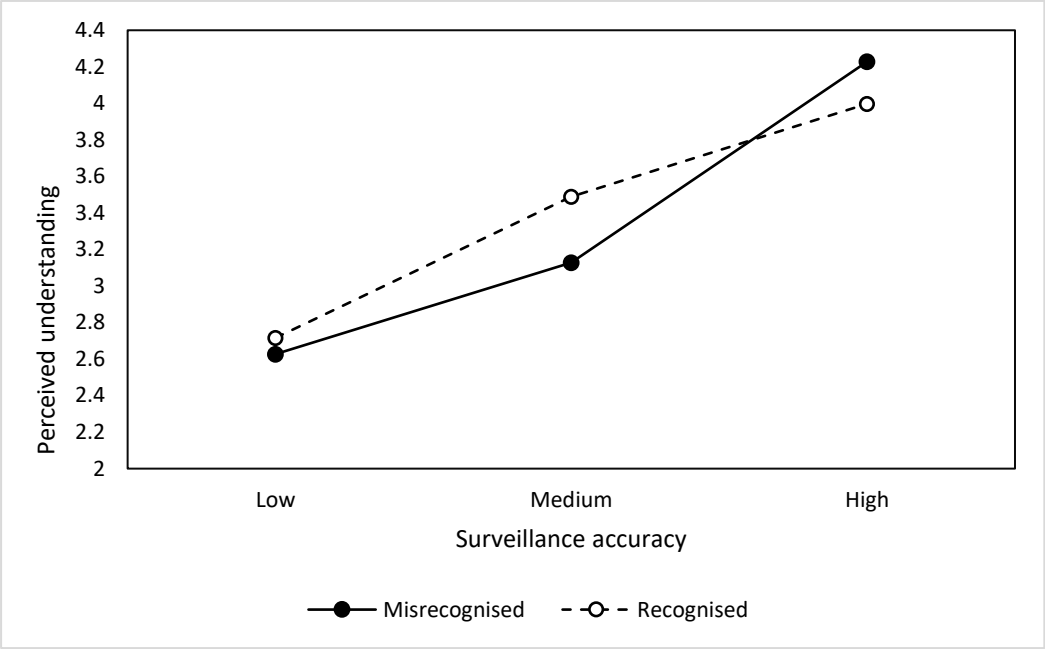


Figure 14. The conditional effect of surveillance accuracy on felt understanding at the two levels of recognition.

Positivity. A significant main effect was found for surveillance accuracy on perceived positivity, $F(2, 388) = 108.29$, $p < .001$, $\eta_p^2 = .358$. Those in the low accuracy condition ($M = 3.17$, $SD = 0.95$) reported significantly less positivity than those in the medium accuracy condition ($M = 4.02$, $SD = 0.94$, p < .001). Surveillance of medium accuracy was associated with significantly less

understanding than high (M = 4.83, SD = 0.87, p < .001). Highly accurate surveillance was associated with significantly more perceived positivity than low (p < .001).

Additionally, a main effect of chronic (mis)recognition was found for perceived positivity, $F(1, 388) = 9.52$, $p = .002$, $\eta_p^2 = .024$. The misrecognised group reported significantly less perceived positivity (M = 3.84, SD = 1.15) than the recognised group (M = 4.16, SD = 1.12).

No interaction was found between surveillance accuracy and chronic (mis)recognition on perceived positivity, $F(2, 388) = 0.23$, $p = .795$, $\eta_p^2 = .001$.

Privacy concern. A 2(chronic (mis)recognition: recognised, misrecognised) X 3 (surveillance accuracy: low, medium, and high) ANOVA was conducted with privacy concern as the dependent variable. No main effect was found for surveillance accuracy on privacy concern, $F(2, 388) = 0.87$, $p = .422$, $\eta_p^2 = .004$. The main effect of chronic (mis)recognition on privacy concerns approached significance, $F(1, 388) = 2.80$, $p = .095$, $\eta_p^2 = .007$. Those in the misrecognised condition (M = 4.79, SD = 1.11) reported marginally less privacy concern than those in the recognised condition (M = 4.97, SD = 1.13).

No interaction was found between surveillance accuracy and (mis)recognition on privacy concern, $F(2, 388) = 1.93$, $p = .147$, $\eta_p^2 = .010$.

Psychological outcomes on feelings towards surveillance. Two multiple regression analyses were conducted to investigate whether privacy concerns and group-based recognition (positivity, distinctiveness, understanding) predicted feelings towards surveillance (positive and negative).

Positive feelings towards surveillance. The overall model was significant and explained 2% of the variance ($R^2_{adj} = .02$, $F(4, 389) = 2.97$, $p = .019$). Results are presented in Table 16.

Of the recognition measures, positivity was the only dimension to predict positive feelings towards surveillance. Greater perceptions of positivity predicted more positive feelings towards surveillance. Privacy concerns did not predict positive feelings towards surveillance.

Table 16. Multiple regression analysis investigating the relationship between psychological outcomes and positive feelings towards surveillance

IV	*b*	β	*t*	*p*
Privacy concern	-.04	-.05	-0.90	.367
Distinctiveness	-.02	-.02	-0.27	.787
Understanding	.01	.02	0.19	.851
Positivity	.14	.16	1.98	.049

Negative feelings towards surveillance. The overall model was marginally significant and explained 1% of the variance (R^2 adj = .01, $F(4, 389) = 2.32$, $p = .057$). Results are presented in Table 17.

Perceived positivity approached significance, with more perceived positivity predicting marginally less negative feelings towards surveillance. Privacy concern did not significantly predict negative feelings towards surveillance.

Table 17. Multiple regression analysis investigating the relationship between psychological outcomes and negative feelings towards surveillance

IV	*b*	β	*t*	*p*
Privacy concern	-.09	-.08	-1.61	.109
Distinctiveness	.01	.01	0.09	.928
Understanding	.01	.01	0.15	.878
Positivity	-.16	-.15	-1.85	.065

Discussion

In Chapters 3 and 4 we argued that evidence of an association between surveillance accuracy and group-based recognition was found (whereas they were not in Study 1) because identity needs were salient (i.e., participants experienced identity threat/misrecognition). However, we did not directly manipulate identity threat/recognition. To address this, the current study manipulated recognition directly by informing Welsh participants that Welsh people were either misrecognised (e.g., perceived as English and national achievements ignored/erased in media and literature) or recognised (e.g., Wales is a celebrated nation that is globally lauded).

If the association between surveillance accuracy and group-based recognition was in turn dependent on salient misrecognition, then the effect of accuracy should have been weaker in the recognition condition (compared to the misrecognition condition), as recognition needs are already met. In contrast, the effect of surveillance accuracy on group-based recognition in the misrecognition condition should have been stronger, as participants in this

condition would not have their recognition needs met and would therefore experience more accurate surveillance as an opportunity to bolster group-based recognition.

The positive pathway: (Mis)recognition does not moderate the association between surveillance accuracy and group-based recognition

The results provided little evidence for an interaction between surveillance accuracy and (mis)recognition. No interaction was found between surveillance accuracy and chronic (mis)recognition on group-based recognition. Instead, we found stronger support for the model proposed in Chapter 1, whereby surveillance of greater accuracy is associated with more group-based recognition *per se*. This effect was found for all recognition dimensions and was irrespective of whether participants believed their group was chronically recognised or misrecognised.

The current results support our broader prediction that accurate surveillance may function as an opportunity for recognition for those who are stigmatised or chronically misrecognised. On the other hand, inaccurate surveillance has the potential to undermine or threaten recognition for groups that already feel recognised. For those in the recognition condition, believing that their group was recognised was not protective against the effects of inaccurate surveillance. As a result, inaccurate surveillance may still function as an identity threat for otherwise well-recognised groups. Indeed, Branscombe et al. (1999) identified four categories of identity threat: categorisation threat, distinctiveness threat, threats to the value of social identity, and acceptance threat. These forms of threat may all be experienced to varying degrees in surveillance contexts. For example, surveillance may inaccurately identify a user as belonging to a specific social group (categorisation threat). This was

illustrated in Stuart and Levine (2017) by a participant who reported unease when mistakenly identified as a gay male: 'But then I started getting adverts for gays all around [location]…and I was like no thanks I am really not interested in that…I was like ah!' (p. 701).

Additionally, research by Patel (2012) highlights the potential for individuals to feel distinctiveness and value threat through inaccurate surveillance. For example, one participant (Alana) found that others perceived her headscarf to signal a terrorist identity: "'oh, she must be a terrorist or hiding something'…for me it's a positive thing and it's about modesty" (p. 228). Here, inaccurate surveillance from the public contributes to both distinctiveness and value threat, whereby Alana felt the Muslim identity was considered synonymous with terrorism (distinctiveness threat) and that a positive aspect of her identity was perceived negatively by others. The current study provides quantitative evidence to support this, as those who believed surveillance was less accurate reported less group-based recognition, suggesting that individuals may experience less accurate surveillance as identity threatening. Thus, the accuracy of surveillance may have the ability to shape group-based recognition, regardless of a group's prior levels of recognition.

Group-based recognition may predict feelings towards surveillance. In turn, we predicted that greater perceptions of group-based recognition would predict more positive and less negative feelings towards surveillance. This was only partially supported by our findings. As expected, a greater belief that one's group was perceived positively by surveillance predicted more positive and (marginally) less negative feelings towards surveillance. However, distinctiveness and understanding did not predict feelings towards surveillance, contrary to expectations.

These findings are not necessarily at odds with the results from previous chapters. For example, in Study 3a understanding did not uniquely predict negative feelings towards surveillance and distinctiveness predicted neither positive nor negative feelings towards surveillance. Additionally, in Study 2c, neither distinctiveness nor understanding uniquely predicted feelings towards surveillance. However, in these studies there were nevertheless strong (and modest yet significant) zero-order correlations between the group-based recognition dimensions and feelings towards surveillance. Therefore, whilst each dimension may not (consistently) uniquely predict feelings towards surveillance, the potential predictive power of the measure as a whole is worth noting here and in the studies mentioned above.

As suggested elsewhere in this thesis, it could be argued that each recognition dimension may vary in importance depending on the group's recognition needs at that time. For example, a prominent stereotype of Welsh people is that they are of lesser intellect and ability compared to other British people, specifically the English. This was illustrated in a survey conducted by the magazine *Maxim,* in which nearly half of non-Welsh British men perceived Welsh people as the least intelligent nationality in the United Kingdom ("Special report Welsh men are 'most stupid'", 1999). Therefore, it could be argued that Welsh people may value positivity to a greater extent than the other recognition dimensions.

It is also worth noting that during data collection the United Kingdom had invoked Article 50 following the European Union referendum and was in the process of leaving the EU. Whilst speculative, it could be argued that during this period the Welsh identity was less central to Welsh people compared to the superordinate British Identity. Therefore, whilst individuals may have still been

susceptible to variations in Welsh recognition, the *consequences* of feeling more or less recognised (as Welsh) may differ. It is possible that whilst surveillance of greater accuracy increased feelings of distinctiveness, individuals may have felt more apathetic towards such increases in group distinctiveness, as their Welsh identity was less salient compared to their British identity at the time of data collection. As this is speculative, further research is needed to explore whether group-based recognition dimensions vary in their psychological consequences depending on the socio-political context.

Alternatively, it could be that participant fatigue may have accounted for some of the null findings here. Participants were asked to read two separate pieces of substantial text before completing the survey. Additionally, the measures pertaining to feelings towards surveillance approached the end of the survey. It could be argued that participants lost interest or struggled to maintain their attention towards the latter half of the survey. This may also account for the null finding between privacy concern and feelings towards surveillance (outlined below).

The negative pathway: Surveillance of greater accuracy was not associated with increased privacy concern

As predicted in our model presented in Chapter 1, we expected more accurate surveillance to be associated with greater privacy concern. Whilst we also manipulated the level of group-based recognition in this study, we did not expect an interaction between surveillance accuracy and recognition, nor a main effect of recognition. No main effect was found for (mis)recognition on privacy concern (although this approached significance) and no interaction was found. However, contrary to our expectations, no main effect was found for surveillance accuracy on privacy concern. It is worth noting that accuracy

perceptions were associated with privacy concern, yet this was in the opposite direction to what was expected; perceiving surveillance as more accurate predicted *less* privacy concern.

A negative association between surveillance accuracy perceptions and privacy concerns was also found in Studies 2b and 3a. As with Study 3a, it could be that as Welsh people are historically stigmatised, accurate representation through surveillance may be considered a fair trade for their privacy. As a result, individuals who perceive a fair trade may experience less concern for their privacy. This was illustrated by Pavone and Esposti (2010), who found that individuals who perceive surveillance as providing some benefit (e.g., safety) are less likely to report privacy concern. In these cases, as surveillance is perceived to serve a purpose and provide benefits to the group, individuals may be less likely to experience privacy concern and instead perceive surveillance as less privacy infringing.

Privacy concern did not predict feelings towards surveillance. We predicted that greater privacy concern would be associated with more negative and less positive feelings towards surveillance. Results did not indicate a significant association between privacy concern and positive nor negative feelings towards surveillance. This does not support our findings from the other studies included in this thesis, all of which indicated a consistent association between privacy concern and feelings towards surveillance.

As mentioned above, it could be that respondent fatigue may account for these null findings. The current study was comparatively longer than the other studies presented in this thesis, as there were two manipulation texts and an additional manipulation check. It could be suggested that as the privacy concern

measure appeared late in the survey, participants may have experienced survey fatigue. Additionally, as the study was conducted online via Prolific Academic, participants were not in the presence of the researcher, which may have reduced investment in participation, particularly towards the end of the survey. Consequently, as our other studies presented in this project have consistently demonstrated an association between privacy concern and feelings towards surveillance, the null result in this case (and elsewhere in the study, as discussed above) may not indicate the absence of an effect.

Limitations and future research

There was no evidence of an interaction between surveillance accuracy and chronic (mis)recognition on group-based recognition. Additionally, Studies 2b and 2c found no interaction between surveiller identity and surveillance accuracy. Together, this indicates that the positive pathway in the predicted model may be true for – and not limited to – groups that already perceive group-based recognition. Nevertheless, as we found some evidence that surveillance accuracy may not provide recognition benefits when recognition needs are met (Study 2a), future research may still benefit from testing the positive pathway within additional group-based contexts where recognition needs vary.

Additionally, positivity was the only recognition dimension to uniquely predict feelings towards surveillance. It is likely that the recognition dimensions cancelled out the effects of one another (at least for positive feelings, as all group-based recognition dimensions had positive and significant zero-order correlations with positive feelings towards surveillance). However, as argued above, positivity may also be comparatively more important for Welsh people than the other dimensions due to the content of Welsh stereotypes and the political climate during data collection. As such, future research should test our

assumptions by recruiting those from other social groups who have different social identity needs compared to the participants in the current study. For example, Hopkins (2011) found British Muslims felt their dual identity was rarely recognised. Participants in this case often reported feelings of misrecognition, as they were often miscategorised as Muslim, which was often synonymous with being foreign. For these individuals, distinctiveness was a salient component of what is meant to experience group-based recognition. Therefore, as different social groups have various identity needs, future research may find that the group-based recognition dimensions have a different relationship with feelings towards surveillance than those found in the current study.

Summary

This study tested whether surveillance accuracy and chronic (mis)recognition have an interactive or additive effect on group-based recognition. Our results did not find evidence for an interaction. Instead, surveillance of greater accuracy was associated with more group-based recognition, irrespective of (mis)recognition condition. These findings build upon those from previous chapters in several important ways. These will be discussed in the following chapter, along with a discussion of potential limitations of the present thesis, avenues for future research, and real-world implications of our findings.

CHAPTER 6

GENERAL DISCUSSION

This thesis has examined the processes behind variation in people's feelings towards algorithmic surveillance. We have provided a social psychological perspective on algorithmic surveillance that contributes to both psychological and digital technology literature. Specifically, we investigated whether surveillance *accuracy* (i.e., the extent to which those surveilled believe surveillance mirrors their own self-concept, including salient social identities) helps to explain variation in feelings towards surveillance through two competing pathways: a positive pathway through group-based recognition, and a negative pathway through privacy concern.

Summary of findings

In Chapter 1 we argued that whilst previous research has explored the negative consequences (both psychological and social) of surveillance, little research has investigated potential positive consequences that may help explain the variation in people's feelings towards surveillance. As surveillance aims to identify aspects of our self which are central to our identity, we argued that (group-based) recognition may serve as a positive outcome of surveillance. Additionally, we highlighted that previous research typically approaches surveillance as a binary concept; the consequences of surveillance are compared to those where surveillance is absent. Whilst this distinction is useful, the current ubiquity of surveillance suggests a more nuanced approach may be more relevant. Specifically, surveillance can vary in its accuracy, whereby the assumptions surveillance makes about users' characteristics may be more or less accurate. Thus, Chapter 1 argued that more accurate surveillance would

be associated with greater privacy concern and (group-based) recognition, and that these would predict more negative and more positive feelings towards surveillance respectively.

The empirical investigation presented in Chapter 2 examined the effects of surveillance at three levels of accuracy (high, medium, and low) on recognition and privacy concern, and whether these psychological outcomes predicted feelings towards surveillance. It is important to note that our first empirical study focussed on individual-based recognition; our approach evolved after Study 1 to explore the effects of surveillance accuracy on *group*-based recognition for reasons that will be explored further below. In Chapter 2 we found some support for the negative pathway: surveillance of high accuracy was associated with more privacy concern than surveillance of medium accuracy; however, this was only true for those who used the internet to a greater extent. Additionally, greater privacy concerns predicted more negative feelings towards surveillance. We also found partial support for the positive pathway; surveillance accuracy was not associated with greater recognition, yet greater recognition predicted more positive feelings towards surveillance.

We concluded in Chapter 2 that our experimental design did not raise specific social identity-related concerns, and in turn did not make group-based recognition needs salient. We argued that this could have accounted for the null effect of surveillance accuracy on recognition, as participants may have believed their recognition needs were met. As such, following Study 1 we aimed to make a specific identity salient by focussing on *social* identity and *group-based* recognition. Consequently, Chapters 3 and 4 aimed to make group-based recognition needs salient by (1) making the identity of the surveiller known as either the ingroup or outgroup (Chapter 3), and (2) recruiting samples

from chronically-misrecognised groups (Chapter 4). Thus, from Chapter 3 onwards we measured *group*-based recognition rather than individual-based recognition.

Positive pathway: Positive feelings towards surveillance through group-based recognition. In Chapter 3, we investigated whether the surveiller's social identity would moderate the association between surveillance accuracy and group-based recognition. We anticipated a linear association between accuracy and group-based recognition when the surveiller belonged to an outgroup, as outgroup audiences typically prompt identity related concerns (Hopkins et al., 2007; Klein & Azzi, 2001; van Leeuwen & Täuber, 2012). In this instance, accurate surveillance may function as a communicative tool through which to garner recognition. We expected the association between surveillance accuracy and group-based recognition to be weaker when the surveiller belonged to the ingroup, as recognition is already implied through shared group membership and therefore surveillance cannot provide any further group-based recognition benefits. In turn, we predicted that greater group-based recognition would predict more positive and less negative feelings towards surveillance.

Chapter 3 provided some support for these predictions. Study 2a found that surveiller identity moderated the relationship between surveillance accuracy and group-based recognition; the linear association between surveillance accuracy and group-based recognition was only present for those surveilled by the outgroup. However, this finding was not replicated by the remaining empirical work in Chapter 3. Instead, we found greater support for independent effects of accuracy and surveiller identity. Surveillance of greater accuracy (either the manipulation itself or accuracy perceptions) was associated with more group-based recognition. Surveiller identity was also associated with

group-based recognition indirectly through trust: the ingroup surveiller was trusted to a greater extent, and greater trust was associated with more group-based recognition. Therefore, Chapter 3 provided evidence for the positive pathway, whereby surveillance of greater accuracy and ingroup surveillance was associated with more group-based recognition, which predicted more positive feelings towards surveillance.

Chapters 4 and 5 also provided support for the positive pathway from accurate surveillance. In Chapter 4 we aimed to make group-based recognition needs salient by recruiting samples from chronically misrecognised groups (surveiller social identity was not manipulated). Study 3a (which sampled people who identified as gay) found that those who perceived surveillance as more accurate were more likely to feel that their group was better recognised. Additionally, Studies 3b and 4 found that participants who believed surveillance was of greater accuracy were also more likely to report greater group-based recognition. In sum, this thesis provides strong evidence that *accurate* surveillance can bolster perceptions of group-based recognition when social identity is salient.

The indirect relationship between surveillance accuracy and feelings toward surveillance through group-based recognition was somewhat less consistent, yet encouraging. Study 3a found an indirect effect between surveillance accuracy and feelings towards surveillance through the positivity dimension of group-based recognition: believing that surveillance was more accurate predicted more perceived group positivity, which in turn predicted more positive and less negative feelings towards surveillance. No indirect effects were found through understanding nor distinctiveness. Study 3b then found an indirect relationship between surveillance accuracy and feelings

towards surveillance through distinctiveness.[36] Surveillance of greater accuracy was associated with a greater perception that one's group is perceived as distinct. In turn, more perceived distinctiveness was associated with more positive and less negative feelings towards surveillance. An indirect relationship was also found through positivity on negative feelings: more accurate surveillance was associated with a greater feeling that one's group is perceived positivity, which in turn predicted less negative feelings towards surveillance. No indirect effect was found through positivity on positive feelings towards surveillance. Therefore, despite some inconsistencies, our findings lend some support to our prediction that surveillance of greater accuracy predicts more positive (and less negative) feelings towards surveillance through increased group-based recognition.

Negative pathway: Negative feelings towards surveillance through privacy concern. This thesis does not provide strong support for the negative pathway, whereby more accurate surveillance was expected to predict more negative and less positive feelings towards surveillance through privacy concern. In Chapter 4, Study 3a found an indirect relationship between surveillance accuracy perceptions and feelings towards surveillance through privacy concern; however, this was in the opposite direction to what was expected. Perceiving surveillance as more accurate predicted *fewer* privacy concerns, which in turn predicted more positive and less negative feelings towards surveillance. Additionally, no direct association was found between surveillance accuracy and privacy concern in the studies in Chapter 3,[37] Study 3b, or in Chapter 5. Consequently, our findings do not support the full negative

[36] In this study the distinctiveness and understanding dimension items were combined.
[37] Studies 2a and 2b found an association between surveillance accuracy *perceptions* and privacy concern, but no effect was found for the accuracy manipulation itself.

pathway of our predicted model. Instead, our findings suggest that surveillance accuracy may have little effect on privacy concern over and above the effect of the *presence* of surveillance

However, we found stronger support for the latter part of the predicted negative pathway; our findings suggest that those who experience greater privacy concern surrounding surveillance are more likely to feel less positively and more negatively towards surveillance. Privacy concern consistently predicted feelings towards surveillance in the expected direction in Chapters 2, 3 and 4. However, the study presented in Chapter 5 did not replicate these findings, as privacy concern did not predict positive nor negative feelings towards surveillance. Nevertheless, the empirical work presented in this thesis overall provides strong support for the predicted association between privacy concern and feelings towards surveillance.

Are group-based recognition benefits through accurate surveillance contingent on misrecognition? In Chapter 2 we found no association between surveillance accuracy and recognition. Here, we suggested that no association was found because social identity concerns were not made salient, and as such, participants may have felt their recognition needs were already met. Our argument was supported by the findings from Chapters 3 and 4, where an association was more consistently found between surveillance accuracy and group-based recognition in contexts where social identity concerns were salient.

It is also important to note that the two studies in Chapter 3 that found a weaker association between surveillance accuracy and group-based recognition (Studies 2a and 2b) relied on psychology student samples. When recruiting students from psychology, it is possible that participants may attempt to guess

the aims of the study or display less engagement with study materials, as they are encouraged to participate in research throughout their studies and thus may experience participation fatigue. In our studies that included samples from the general population, we found the effect of surveillance accuracy on group-based recognition to be stronger. Thus, taken together we argued that social identity concerns may need to be salient for those surveilled to achieve group-based recognition benefits.

To test whether group-based recognition from accurate surveillance is indeed contingent on social identity concern (misrecognition), in Study 4 (Chapter 5) we manipulated chronic (mis)recognition directly before presenting participants with the surveillance accuracy manipulation. We predicted that an association between accuracy and group-based recognition would only be found for those who believed their group was already misrecognised. We did not predict an association for those who believed their group was recognised, as accurate surveillance was unlikely to provide any further recognition benefits. Contrary to our expectations, chronic (mis)recognition was not found to moderate the association between surveillance accuracy and recognition. Instead, surveillance of greater accuracy led to more group-based recognition for those in both recognition conditions.

Additionally, in Chapter 3, only Study 2a found any evidence that surveiller identity moderated the effect of surveillance accuracy on group-based recognition. Specifically, only those surveilled by the outgroup (and not the ingroup) perceived group-based recognition benefits from accurate surveillance. Studies 2b and 2c did not find that surveiller identity moderated the relationship between surveillance accuracy and group-based recognition. Together this may suggest that chronic misrecognition/social identity concern is not necessary for

individuals to experience group-based recognition through accurate surveillance. Instead, the effect of surveillance accuracy on group-based recognition may be more pervasive than we first anticipated. Individuals may simply require a social identity to be salient to achieve group-based recognition, and group-based recognition benefits may be achieved irrespective of a group's perceived status or appraisal.

Contributions of the present thesis

Previous research has established a body of evidence that suggests individuals experience negative outcomes from surveillance, predominantly in the form of privacy concern (e.g. Almuhimedi et al., 2015; Dinev & Hart, 2004; Möllers & Hälterlein, 2013). Whilst the negative outcomes of surveillance are well researched, there is little evidence that addresses the ambivalence individuals often feel towards surveillance (Ellis et al., 2013; Graham & Wood, 2003). As discussed in Chapter 1, public reactions towards surveillance systems are typically variable, such as the recent example of the public response to Facebook's acquisition of WhatsApp and the subsequent sharing of data (Tech Crunch, 2016). Public outcry followed the acquisition, yet Facebook's users continued to rise (a phenomenon identified as the privacy paradox; Barnes, 2006; Norberg et al., 2007). In this thesis we aimed to explore the processes underlying this variation in four key ways: (1) by manipulating surveillance accuracy; (2) examining positive outcomes of surveillance in the form of group-based recognition; (3) examining the role of *social* identity within surveillance contexts (rather than individual/personal identity-based approaches); and (4) by examining the link between surveillance accuracy and privacy concern.

The role of accuracy. Firstly, we have gone beyond the binary distinction of surveillance as either present or absent by manipulating surveillance *accuracy*. As discussed earlier in this thesis, surveillance accuracy here pertains to the extent to which individuals believe surveillance mirrors one's own self-concept, including salient social identities. Therefore, surveillance accuracy is the subjective appraisal of the user (and may thus deviate from the surveiller's concept or measurement of accuracy). Previous literature has typically explored the consequences of surveillance by comparing its effects to contexts without surveillance (e.g. Blackwood et al., 2015; Dawson et al., 2005; Marthews & Tucker, 2017; McDonald & Cranor, 2010; Oulasvirta et al., 2012; Pavone & Esposti, 2010). In this thesis we have argued that surveillance – particularly algorithmic surveillance – is more nuanced and its perceived accuracy can be highly consequential. In Chapter 1 we outlined how the quantity of data analysed can contribute to variations in surveillance accuracy (Maass, 2015) and that individuals are often aware of – and have opinions towards – surveillance accuracies and inaccuracies (Ur et al., 2012). Thus, we explored how variations in surveillance accuracy affect psychological outcomes and subsequent feelings towards surveillance. Indeed, here we have demonstrated that surveillance accuracy is quite consistently associated with positive psychological outcomes in the form of group-based recognition benefits.

Additionally, we found evidence that surveillance accuracy is not consistently associated with more privacy concern. Conversely, we found that surveillance of higher accuracy led to *fewer* privacy concerns in some cases. As a result, we demonstrate in this thesis the importance of going beyond the present/absent distinction in surveillance literature, as nuance in surveillance

accuracy may determine how people respond to surveillance technologies. This also highlights that the negative outcomes of surveillance already highlighted in the literature, such as chilling effects (Marthews & Tucker, 2017; Penney, 2016; Stoycheff, 2016), lack of perceived control (Eslami et al., 2015; Garrido, 2015) and privacy concern (Almuhimedi et al., 2015; Möllers & Hälterlein, 2013) may be worth revisiting within the context of surveillance accuracy, as our findings suggest that outcomes may differ depending on how accurate participants believe surveillance to be.

Positive psychological outcomes in the form of group-based recognition. Secondly, we have examined potential *positive* outcomes of surveillance in the form of group-based recognition. Within this thesis we have found that *accurate* surveillance has the potential to provide groups with increased recognition. In *The presentation of self in everyday life,* Goffman argues that individuals strive to be considered in a way that aligns with their own self concept, and that we engage in identity performances in order to achieve this. Indeed, research has found that individuals who do not feel recognised will engage in behaviour to address these misconceptions (Klein & Azzi, 2001). Our findings here extend this literature by demonstrating that perception *accuracy* (i.e. the alignment of others' perceptions with one's self concept) is an integral antecedent of group-based recognition, and that recognition is less likely if individuals believe they are perceived inaccurately.

Additionally, this thesis has highlighted that group-based recognition online may be possible outside of peer-to-peer networks. Previous literature has highlighted the use of online media to garner recognition from peers. For example, Kennedy (2006) found that disadvantaged women perceived their personal online homepages as a platform on which to gain recognition from

other online users. This mirrors users' perceptions of social media sites, such as Facebook. Steeves (2016) found that adolescents use Facebook to curate their image in a way that increases recognition from their social network. The current thesis extends this by illustrating that surveillance may provide internet users with an additional vehicle to bolster recognition, even when surveillance is not conducted by a peer or when the identity of the surveiller is unknown. Additionally, whilst social media sites such as Facebook require users to actively build their profile, algorithmic surveillance is unique in that an individual's profile is built indirectly through their general engagement online. Consequently, our findings suggest that (accurate) surveillance can provide individuals with group-based recognition from an abstract or unknown audience, which is comparatively passive to the more active 'performance' that is required in other social contexts.

Furthermore, this thesis demonstrates that the degree to which individuals experience group-based recognition from surveillance may contribute to their feelings towards it. As mentioned elsewhere in this thesis, the processes underlying people's feelings towards surveillance are rarely examined. Positivity and/or negativity is often assumed from the outcomes under investigation (e.g., Dinev et al., 2008). Whilst intuitive, we demonstrate here that greater perceptions of group-based recognition have the potential to increase positive (and reduce negative) feelings towards surveillance.

It is important to note, though, that certain dimensions of recognition appeared to more consistently predict feelings towards surveillance, namely positivity. Indeed, previous literature has argued that aspects of one's group identity are more central/salient than others depending on the context or social pressures (Kelman, 2004). For example, in Barreto et al.'s (2003) research,

dual nationality (Dutch-Portuguese) participants were more likely to express their Dutch identity when anonymous to a Dutch audience compared to when they were identifiable. The authors argued that their claim to the Dutch identity was weakened when identifiable to a Dutch audience, as the legitimacy of this claim is more likely to be questioned than when anonymous. Thus, contextual pressures – in this case, identifiability to the assumed audience – modified which aspects of participant's identity were salient or appropriate to display.

Our findings also suggest that identity needs may vary between groups and contexts. For example, in Study 3a we found that positivity (but not distinctiveness) predicted more positive feelings towards surveillance. It could be argued that for those identifying as gay, being perceived positively is more central to their identity than being considered distinct. As such, increases in distinctiveness may be less likely to affect feelings towards surveillance, as it is less central to their social identity. Here, it is possible that increased group-based recognition does not always predict feelings towards surveillance, as groups may value each recognition dimension differently depending on the context, and certain recognition dimensions may be more fundamental generally to the group's identity than others. However, as discussed elsewhere in this thesis, an alternative and perhaps more likely explanation may be that the dimensions of group-based recognition cancelled out the effects of one another. Instead, group-based recognition *overall* may consistently predict feelings towards surveillance in ways that are not attributable to any given dimension of recognition. Returning to the SIT perspective, the importance is being seen as positively distinct, and not just as distinct.

Chapters 3 and 5 also suggest that accurate surveillance may provide recognition benefits even in contexts where recognition needs are already met.

In Studies 2b and 2c, group-based recognition was increased by accurate surveillance (or was predicted by perceptions of surveillance accuracy; Study 2b), even when surveillance was conducted by the ingroup. Additionally, in Chapter 5 we found that individuals who felt that their ingroup was recognised still received recognition benefits from accurate surveillance. This contradicts previous research which finds individuals are more receptive to opportunities which allow them to challenge *outgroup* perceptions, as individuals wish to challenge negative metastereotypes (van Leeuwen and Täuber, 2012).

Conversely, when in the presence of the ingroup, individuals are less likely to engage in behaviour that might strengthen recognition (Hopkins et al., 2007; Klein & Azzi, 2001; van Leeuwen & Täuber, 2012), as the ingroup is not assumed to hold negative stereotypes about the group (Sigelman & Tuch, 1997; Vorauer et al., 1998 Finkelsteinet al., 2013). Instead, the ingroup is often a fundamental source of group-based recognition; this was evidenced by Neville and Reicher (2011), who found that football supporters received high levels of group-based recognition from fellow fans. For example, one participant explained that '[in the crowd] you're not alone…there are other people that believe in what you believe in and which clearly is always a reassuring thing' (p. 385). Another participant described being part of an ingroup as 'everyone around you is singing from the same hymn sheet' (p. 384).

Together, this suggests that recognition needs are already met when in the presence of the ingroup, whereas recognition is not assumed from outgroup audiences. Whilst our findings do not necessary align with this literature, it could be argued that group-based recognition can be possible from more accurate ingroup surveillance, as the ingroup is trusted to a greater extent. For example, Chapter 3 highlighted the importance of trust, as trust mediated the association

between surveiller identity and group-based recognition. The ingroup was typically trusted to a greater extent, and greater trust predicted more group-based recognition. Trust is a central concept in algorithmic surveillance research, as data can easily be manipulated or misinterpreted (O'Neil, 2016). Therefore, group-based recognition may still be possible through accurate surveillance from the ingroup, as the ingroup is afforded greater trust when handling and interpreting personal data.

Conceptualising group-based recognition. Thirdly, this thesis contributes to both psychology and technology literature by examining *group-based* recognition in surveillance contexts. Previous literature exploring recognition online has typically focussed on individual-based recognition or looks at recognition generally without focussing on a specific aspect of an individual's identity. For example, Steeves and Bailey (2016) talk broadly about recognition of an individual's 'persona', where participants refer generally to 'you' and 'yourself' when discussing peer-to-peer surveillance and recognition.

Whilst it is important to explore how individuals conceptualise and present themselves more generally online, the role of *social* identities may be especially prominent in online contexts. According to the SIDE model, individuating characteristics may become less salient in online settings (Lea & Spears, 1991; Reicher et al., 1995). As such, social identities are emphasised, which can heighten stereotyping and group-normative behaviour (Postmes & Spears, 2002; Spears et al., 2002). Consequently, group-based processes may be more pronounced in online settings, as individuating information is obscured. Our findings support the importance of a social identity approach in online research, as the extent to which individuals believed their *group* identity was recognised in part determined their feelings towards surveillance. This

illustrates that internet users are sensitive to group-based processes online, and that this in turn can inform how they appraise online platforms and technologies.

Additionally, we have laid the foundations for conceptualising group-based recognition more generally. As discussed in Chapter 1, recognition (both individual and group-based) is rarely defined in previous research (Bartelson, 2013). A key aim of this thesis was to present a clear definition of group-based recognition so that it may be more reliably assessed within this thesis and going forward. Whilst our definition and measurement of group-based recognition evolved throughout this project, we encourage others examining group-based recognition to continue to develop our measure presented in this thesis.

Negative psychological outcomes in the form of privacy concern. Lastly, our predicted model suggested that surveillance of greater accuracy would be associated with higher privacy concern. Our findings presented in this thesis do not provide strong support for this prediction. Only Study 1 found an association between surveillance accuracy and privacy concern (for high internet use), as greater accuracy predicted more concern. However, Studies 2b, 3a and 4 found that perceiving surveillance as more accurate predicted *less* privacy concern. The remaining studies also found no association between accuracy nor accuracy perceptions on privacy concern. Whilst these findings are encouraging and suggest surveillance accuracy *may* be associated with privacy concern in some contexts, we suggest that the presence of surveillance *per se* is likely to be a stronger predictor of privacy concern in comparison to surveillance accuracy.

At first glance, our inconsistent findings here do not support previous literature. In Chapter 1 we presented research which would suggest individuals

may feel more concerned for their privacy when surveillance is highly accurate. For example, in Ur et al. (2012) a participant expressed that '…I notice that when I look at an email, the ad at the top seems to cater to what I'm looking at, and I just think that might be an invasion of privacy.' (p. 5). However, it could be argued that the accuracy of surveillance noted by participants in these studies may merely reflect their awareness of it. Many individuals do not identify adverts online as a form of surveillance or behavioural monitoring unless those adverts are clearly tailored to them or they are explicitly informed (Ur et al., 2012). Indeed, in Almuhumedi et al.'s (2015) study, individuals only reported concern for their privacy when they received nudges each time an app on their phone accessed sensitive personal data. As a result, it is difficult to distinguish the potential differing effects of surveillance presence and surveillance accuracy in these studies. In these cases, surveillance accuracy and presence are not experimentally manipulated, thus any effects of accuracy and salience may be confounded.

By contrast, the presence of surveillance was constant between accuracy conditions across the studies in this thesis. Our studies also illustrated a trend whereby privacy concern did not differ across surveillance accuracy conditions. Therefore, this thesis suggests that surveillance accuracy may have little effect on privacy concern over and above the presence of surveillance. Previous literature that suggests an effect of surveillance accuracy may instead demonstrate that it is a heightened awareness of surveillance that results in greater privacy concern.

Perhaps unsurprisingly, we found strong evidence that increased privacy concern predicts less positive and more negative feelings towards surveillance. Research exploring the privacy paradox finds that despite privacy concern,

individuals continue to engage with surveilling online platform (Barnes, 2006; Norberg et al, 2007; Spiekermann et al., 2001). Our findings add to this body of work, as we demonstrate that individuals who feel concern for their privacy *and in turn* feel more negatively towards it may also continue to engage with surveilling organisations.[38] Thus, individuals may feel animosity towards platforms yet maintain online engagement.

Additionally, this thesis demonstrates that those who feel a concern for their privacy have greater intentions to change their online behaviour (Study 2a), and feel more negatively towards surveillance (Studies 1, 2c, 3a, and 3b). This challenges privacy paradox research, which suggests that individuals are not motivated to change their online behaviour despite privacy concern, as users feel mostly apathetic towards surveillance (Hargittai & Marwick, 2016). Instead, the findings from this study suggest that there are other explanations for why individuals do not protect their online data. For example, previous research has shown that people are unlikely to change their online behaviour (despite privacy concern) because they lack technical knowledge (Tene & Polonetsky, 2014) or social and economic pressures discourage disengagement (Welinder, 2012; Acquisti et al., 2012). Therefore, as we found that those concerned for their privacy feel negativity towards surveillance and intend to change their behaviour online, the failure to do so would suggest reasons other than user apathy.

Strengths, limitations and directions for future research

The studies presented in this thesis have several key strengths. Firstly, we have taken a novel approach by examining the positive outcomes of

[38] Whilst we did not take a behavioural measure of online engagement, privacy paradox literature strongly suggests that people do not change their behaviour despite concern for privacy.

algorithmic surveillance, as well as the more established negatives outcomes. By doing so, we have been able to develop a clearer picture as to why feelings towards algorithmic surveillance may vary. Secondly, we have gone beyond the distinction of surveillance as merely either present or absent by examining the effects of surveillance accuracy. Arguably, this makes our current work more relevant considering the current digital landscape, whereby the ubiquity of surveillance suggests a more nuanced approach is necessary. Additionally, we have tested our predicted model within a variety of social groups and identities. As social groups may have different relationships with surveillance and may also have varying recognition needs, our approach allowed us to identify ways in which groups' perspectives on surveillance may differ.

Despite this, it is prudent to identify some general limitations within this project. Whilst Chapter 3 did not find strong evidence for a moderating effect of surveiller identity, we predominantly relied on intergroup contexts that were relatively benign. Studies 2a and 2b in Chapter 3 described surveillance as being conducted by either the Psychology or the Biosciences Department. This intergroup context may not have produced the degree of identity threat necessary for a moderating effect of surveiller identity to occur, for instance. We may therefore have found greater evidence of a moderating effect of surveiller identity if the outgroup represented a greater threat to one's identity. Consequently, future research exploring surveillance processes within an intergroup context should endeavour to recruit those belonging to groups with historically contentious relations.

Furthermore, prior research has found that identity concerns and impression management only occur when metastereotypes are made salient (van Leeuwen & Täuber, 2012). Making metastereotypes explicit may have

strengthened the effect of surveiller identity and its potential moderator role. Thus, future work examining whether surveiller identity moderates the effect of surveillance accuracy on group-based recognition may benefit from making metastereotypes salient. Lastly, future replications should avoid psychology student samples, as this increases the likelihood of participants second-guessing the study aims and predictions. We may be more confident in our findings that surveiller identity does not appear to moderate the association between surveillance accuracy and recognition when these limitations have been addressed.

Based on the findings from Chapters 3 and 4, Chapter 5 aimed to test our assumption that misrecognition was necessary for surveillance accuracy to improve group-based recognition; however, our findings did not support this. This suggests that the positive pathway (more accurate surveillance predicts more positive (and less negative) feelings towards surveillance through group-based recognition) is true for both chronically-recognised and misrecognised groups. Nevertheless, future research may benefit from strengthening the recognition manipulation to further test this. To explore the potential moderating effect of (mis)recognition, future work could employ a quasi-manipulation of group-based recognition. This may be operationalised by comparing the effects of surveillance accuracy between two different pre-existing social groups: a chronically recognised group and a chronically misrecognised group, rather than manipulating (mis)recognition within the same social group. However, it is also worth noting that quasi-manipulations such as these may introduce confounds that are typically avoided with a direct manipulation, which was the main reason a direct manipulation was adopted in Study 4. Future work adopting a quasi-manipulation approach should endeavour to control for

potential confounds to provide a valid test of whether misrecognition is necessary to experience recognition benefits from accurate surveillance.

Additionally, whilst this project recruited participants from a variety of social groups, future work should endeavour to explore these processes within groups that have different societal experiences than those examined here. For example, none of the groups included in this project have historically experienced supravisibility. Other social groups, such as those identifying as Muslim, may have a different relationship with surveillance and visibility. Since 9/11, those identifying as Muslim have been subject to intense surveillance practices by both the media and government agencies (Spalek & Lambert, 2007). For groups that experience supravisibility in this way, an association between surveillance accuracy and group-based recognition may be weaker, as the source of surveillance is distrusted (Ali, 2016).

Furthermore, within this project we predominantly focussed on algorithmic surveillance in general and did not compare/contrast the outcomes of government versus commercial surveillance, for instance. This was not the focus of the present thesis, and data streams are often shared between various sources of surveillance (including state and commercial). However, evidence suggests that some individuals may have a greater trust in government surveillance, as only those considered criminals are assumed to be under scrutiny (Ellis et al., 2013; Pavone & Esposti, 2010). Therefore, future work may benefit from comparing the outcomes of surveillance conducted by government and commercial sources.

Future work may also benefit from going beyond the model presented here by exploring the implications of group-based recognition online aside from

feelings towards surveillance. For example, increased group-based recognition from accurate surveillance may reinforce one's social identity. In turn, individuals may be more likely to behave in ways that correspond with their social identity. For example, Summers, Smith and Reczek (2016) found that participants who were shown adverts for green products subsequently considered themselves more environmentally friendly than those not shown green adverts. Therefore, future work could explore the implications of increased group-recognition online and how this affects self-perception and behaviour.

Practical implications

Aside from the theoretical contributions of this thesis, here we offer some real-world implications of our empirical findings. Notable works such as those by Cathy O'Neil (2016) and Shoshana Zuboff (2019) highlight how social groups are affected by those conducting algorithmic surveillance, in that current surveillance practices (surveillance/data capitalism) have contributed - and are likely to continue to do so - to social inequality and injustice (West, 2017). Whilst O'Neil and Zuboff focus on the social and economic consequences of surveillance, we extend this by demonstrating the psychological consequences of data surveillance. Perhaps the most novel finding of this thesis is the potential for accurate surveillance to foster group-based recognition. From this, we add to the responsibilities held by those who program and conduct algorithmic surveillance. Considering the ubiquity of algorithmic surveillance (Lee, 2015), our findings suggest that those conducting surveillance online take into consideration how accurately their targeted material represents social groups. The accuracy of surveillance and the resulting targeting material has the potential to impact how groups believe they are perceived, and in turn how

they feel towards online platforms and systems. This may have broader implications for groups' collective self-esteem, wider intergroup relations, and how certain groups engage digitally. Indeed, regulating bodies have begun to take these processes into account. In June 2019, the UK's advertising watchdog introduced a ban on adverts featuring gender stereotypes ("'Harmful' gender stereotypes in adverts banned", 2019), which included those shown online and on social media. Based on the findings of this thesis we encourage further consideration of the role of psychological processes in targeted material, and specifically encourage organisations to consider the implications of how accurately social groups are presented in targeted content.

Additionally, our findings suggest that an increase in algorithm accuracy (in the specific sense of whether the portrayal of a group aligns with the group members' self concepts) is unlikely to increase negative psychological outcomes in the form of privacy concern over and above the concern already felt by the presence of surveillance. Therefore, our findings suggest that organisations consider the appropriateness and value of surveillance in online contexts, as the mere presence of surveillance is likely to heighten privacy concern and in turn increase animosity towards those systems. As our findings suggest that this is irrespective of how accurately social groups are presented in targeted material, surveilling organisations may benefit from considering whether the perceived benefits of surveillance outweigh the cost of increased privacy concern.

We have illustrated in this thesis that an increase in group-based recognition without a simultaneous increase in privacy concern may lead individuals to feel more favourably towards surveillance. This may initially raise ethical concerns for some, as approaches that encourage favourability towards

surveillance may resemble the manipulation techniques surveillance is often criticised of (Costa & Halpern, 2019). An alternative perspective is that surveillance which results in less privacy concern and greater group-based recognition offers a fairer exchange, whereby the interests of both surveillance capitalism and the consumer are met. For example, some internet users perceive tangible benefits from targeted material in the form of shopping discounts (Ur et al., 2012). It is important to note that our findings do not delineate the differences between 'good' or 'bad' surveillance, and we do not claim that our results aid in qualifying surveillance practices. Instead, we take a techno-positive perspective, whereby surveillance is neither inherently good nor bad. It is the duty of those using technology that harnesses psychological processes to do so responsibly.

In light of this, whilst we frame group-based recognition as a positive psychological outcome of accurate surveillance, we do not deny that there may be negative *social* consequences of group-based recognition in online contexts. For example, an increase in group-based recognition within the current framework of surveillance may produce long-term negative consequences that have not been explored in this thesis. For example, Neville and Reicher (2015) demonstrated that individuals feel that their beliefs and attitudes are emboldened when experiencing group-based recognition: "you're not alone in your struggle basically for what you believe in…you realise to yourself 'yes, I probably am actually right'" (p. 385). This is particularly true when targeted material extends to political and cultural propaganda.

Highly-accurate surveillance that fosters group-based recognition in this context may also contribute to filter bubbles, whereby belief systems become ever-more entrenched (Bozdag & van den Hoven, 2015). Indeed, filter bubbles

are believed to contribute to the zeitgeist, social division, and interfere with national elections and referendums (Cadwalladr, 2019). This is an issue that is far too broad and complex to be addressed here. However, some research suggests that the social issues resulting from filter bubbles may be mitigated when users are given the option to opt in or out of such systems. When given the choice to receive non-filtered content, individuals consume an equal amount of belief-affirming and disconfirming information (Gladfelter, 2018). Using this approach, individuals may harness the potential benefits of targeted filtered material if they wish, yet maintain the freedom to diversify their content at any given time. Alternatively, individuals may choose to opt out of behavioural tracking altogether. This gives those online the choice to consume targeted material when there is a preference for it, without the totalitarian filtering of their content.

Additionally, as with many theoretical models, the positive pathway outlined in this thesis may not be generalisable to all groups and contexts. For example, it is necessary for some groups to conceal their social identity for safety reasons and to avoid discrimination (Kelly & McKillop, 1996; Rossman, Salamanca, & Macapagal, 2017), even if doing so can result in poorer psychological outcomes (Newheiser & Barreto, 2014). As such, individuals may be less likely to experience positive psychological outcomes or feel positively towards surveillance when accurate surveillance makes users feel as though a concealed identity is exposed. In this instance, an individual may feel their personal safety is jeopardised. For example, in October of 2019, Ugandan members of parliament petitioned for homosexual acts to be punishable by death (Burke & Okiror, 2019). Those identifying as gay in Uganda (and in other countries where homosexuality is criminalised) would be unlikely to experience

accurate surveillance more positively (or less negatively), as accurate surveillance poses a significant risk to one's safety. In sum, there may be some circumstances where the positive pathway may not be as strong when its ability to recognise someone as a member of that group makes them vulnerable to negative consequences.

However, it is also important to distinguish between how an *individual* may feel towards the exposure of their group membership, and the *collective* experience of group-based recognition as part of a social movement or campaign. Surveillance accuracy as we define it here may still be part of a movement or solution that strives to change society's perceptions of the ingroup. The struggle for rights at a collective level typically requires accuracy as a basis of recognition (Blackwood et al., 2013; Hopkins, 2011) precisely when the recognition of individuals' stigmatised identity is highly threatening. As such, if a social movement is already established, in which individuals feel greater personal safety and support as a collective, accurate surveillance may be an effective component of a broader campaign which aims to change attitudes towards the ingroup.

It is also worth noting that the findings of this thesis and the implications discussed here may only occur if individuals are aware of surveillance. Within each of our studies we provided participants with an explicit description of algorithmic surveillance and online surveillance practices. However, without explicit notification, individuals are often unaware of surveillance practices and those that are aware may be unsure how surveillance affects them (Ur et al., 2012). Even when users are informed of surveillance through terms and conditions, the length and complexity of these terms mean that users maintain low comprehension of surveillance implications (Felt, Ha, Egelman, Haney,

Chin, & Wagner, 2012). As such, the predicted model in this thesis may only apply in contexts where individuals are aware of surveillance and its outcomes. Results may differ in circumstances where participants are less aware; for example, individuals are unlikely to perceive variation in surveillance accuracy if they are not aware of surveillance in the first place, and are unlikely to perceive surveillance accuracy as consequential if they do not believe they are under surveillance.

Conclusion

Current narratives surrounding surveillance centre on its negative outcomes, such as those relating to privacy concern. Whilst vital, this approach fails to explain the variability in the public's attitude towards surveillance. This thesis has elucidated some of the processes that may account for this variation; specifically, we find that accurate surveillance can provide groups with increased group-based recognition. Whilst previous research argues that the continued use of surveilled platforms is due to user apathy, we propose an alternative explanation that users may be less likely to withdraw from these platforms, as they may provide social identity-related benefits. Our work has also highlighted the utility of exploring the nuance of surveillance by going beyond the dichotomy of surveillance as either present or absent. By doing so, we have been able to illustrate identity-related processes that contribute to the publics' perception of algorithmic surveillance. By gaining a better understanding of the identity-related processes surrounding surveillance we are able to further highlight the responsibility of those that collect our data. It is the role of the scientific community to equip society with a better understanding of these systems. Only then can we effectively challenge these models and hold the panoptic gaze accountable.

REFERENCES

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*(2), 160-174.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). Retrieved from http://journals.uic.edu/ojs/index.php/fm/article/view/2142/1949

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology*, *86*(4), 797-804.

Ali, A. I. (2016). Citizens under suspicion: Responsive research with community under surveillance. *Anthropology & Education Quarterly*, *47*(1), 78-95.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., ... & Agarwal, Y. (2015, April). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 787-796). Retrieved from http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/home/ftp/isr2014/CMU-ISR-14-116.pdf

Altman, I. (1975). *The environment and social behaviour*. Monterey, CA: Brooks/Cole.

Alvídrez, S., Piñeiro-Naval, V., Marcos-Ramos, M., & Rojas-Solís, J. L. (2014). Intergroup contact in computer-mediated communication: The interplay of a stereotype disconfirming behavior and a lasting group identity on

reducing prejudiced perceptions. *Computers in Human Behavior*, 52, 533–540.

American Civil Liberties Union (n.d.). End mass surveillance under the Patriot Act. *American Civil Liberties Union.* Retrieved from https://www.aclu.org/issues/national-security/privacy-and-surveillance/end-mass-surveillance-under-patriot-act

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479-497.

Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. *National Bureau of Economic Research.* Retrieved from https://www.nber.org/papers/w23488.pdf

Bachmann, A. S., & Simon, B. (2014). Society matters: The mediational role of social recognition in the relationship between victimization and life satisfaction among gay men. *European Journal of Social Psychology*, *44*(3), 195-201.

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication & Society*, *12*(5), 639-657.

Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, *51*(1), 87-106.

Barnes, S. B. (2006). A privacy paradox: Social networking in the Unites States. *First Monday, 11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

Barreto, M., Ellemers, N., & Banal, S. (2006). Working under cover: Performance-related self-confidence among members of contextually

devalued groups who try to pass. *European Journal of Social Psychology*, *36*(3), 337-352.

Barreto, M., Spears, R., Ellemers, N., & Shahinper, K. (2003). Who wants to know? The effect of audience on identity expression among minority group members. *British Journal of Social Psychology*, *42*(2), 299-318.

Bartelson, J. (2013). Three concepts of recognition. *International Theory*, *5*(1), 107-129.

Baumeister, R. F. (1982). A self-presentational view of social phenomena. *Psychological Bulletin*, *91*(1), 3-26.

BBC (2004, October 5). *Eurocrats leave Wales of EU map.* Retrieved from http://news.bbc.co.uk/1/hi/wales/3715512.stm.

Berger, J., & Heath, C. (2007). Where consumers diverge from others: Identity signaling and product domains. *Journal of Consumer Research*, *34*(2), 121-134.

Blackwood, L., Hopkins, N., & Reicher, S. (2013). I know who I am, but who do they think I am? Muslim perspectives on encounters with airport authorities. *Ethnic and Racial Studies*, *36*(6), 1090-1108.

Blackwood, L., Hopkins, N., & Reicher, S. D. (2015). 'Flying while muslim': Citizenship and misrecognition in the airport. *Journal of Social and Political Psychology*, *3*(2), 148-170.

boyd, D. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence*, *14*(1), 13-20.

boyd, D. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

Boyer, C. (2017). *Examining the extent and impact of surveillance on animal rights activists* (Master's thesis, University of Nevada, Las Vegas, USA). Retrieved from https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3951&context=thesesdissertations

Bozdag, E., & van den Hoven, J. (2015). Breaking the filter bubble: Democracy and design. *Ethics and Information Technology*, *17*(4), 249-265.

Branscombe, N. R., Ellemers, N., Spears, R., & Doosje, B. (Eds.). (1999). The context and content of social identity threat. In *Social identity: Context, commitment, content*, (pp. 35-58). Oxford, England: Blackwell Science.

Brashear, T. G., Boles, J. S., Bellenger, D. N., & Brooks, C. M. (2003). An empirical test of trust-building processes and outcomes in sales manager-salesperson relationships. *Journal of the Academy of Marketing Science*, *31*(2), 189-200.

Breen, J. (2018, October 17). Baroness Tanni Grey Thompson honoured with lifetime achievement award. *The Northern Echo.* Retrieved from https://www.thenorthernecho.co.uk/news/local/teesvalley/17974585.baroness-tanni-grey-thompson-honoured-lifetime-achievement-award/

Brewer, M. B. (1979). In-group bias in the minimal intergroup situation: A cognitive-motivational analysis. *Psychological Bulletin*, *86*(2), 307-324.

Brewer, M. B. (1999). The psychology of prejudice: Ingroup love and outgroup hate? *Journal of Social issues*, *55*(3), 429-444.

Brewer, M. B., & Campbell, D. T. (1976). *Ethnocentrism and intergroup attitudes: East African evidence.* New York, NY: SAGE.

Brighenti, A. (2007). Visibility: A category for the social sciences. *Current Sociology*, *55*(3), 323-342.

Bright Horizons. (n.d.). *Cookie policy*. Retrieved from https://www.brighthorizons.co.uk/information/cookie-policy

Brown, I. (2013). How will surveillance and privacy technologies impact on the psychological notions of identity? In *Future identities: Changing identities in the IK – the next 10 years.* Oxford Internet Institute, commissioned by the UK Government's Foresight Project: Government office for science. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.564.4095&rep=rep1&type=pdf

Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, *14*(7), 1164-1180.

Burke, K. (1969). *A grammar of motives* (3rd ed.). Berkeley, CA: University of California Press.

Burke, J. & Okiror, S. (2019, October 15). Ugandan MPs press for death penalty for homosexual acts. *The Guardian.* Retrieved from https://www.theguardian.com/world/2019/oct/15/ugandan-mps-press-for-death-penalty-for-homosexual-acts

Cadwalladr, C. (2019, April). *Facebook's role in Brexit – and the threat to democracy* [Video file]. Retrieved from https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy/up-next?language=en

Cahn, D. D. (1990). Perceived understanding and interpersonal relationships. *Journal of Social and Personal Relationships*, *7*(2), 231-244.

Campbell, D. E., & Wright, R. T. (2008). Shut-up I don't care: Understanding the role of relevance and interactivity on customer attitudes towards repetitive online advertising. *Journal of Electronic Commerce Research*, *9*(1), 62-76.

Caprara, G. V., Barbaranelli, C., Steca, P., & Malone, P. S. (2006). Teachers' self-efficacy beliefs as determinants of job satisfaction and students' academic achievement: A study at the school level. *Journal of School Psychology*, *44*(6), 473-490.

Chang, A. (2018, May 2). 'The Facebook and Cambridge Analytica scandal, explained with a simple diagram'. *Vox*. Retrieved from https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), 395-416.

Chrobot-Mason, D., Button, S. B., & DiClementi, J. D. (2001). Sexual identity management strategies: An exploration of antecedents and consequences. *Sex Roles*, *45*(5-6), 321-336.

Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance & Society*, *15*(5), 609-625.

Clarke, L. H., & Griffin, M. (2008). Visible and invisible ageing: Beauty work as a response to ageism. *Ageing & Society*, *28*(5), 653-674.

Cohen, N. S. (2008). The valorization of surveillance: Towards a political economy of Facebook. *Democratic Communiqué*, *22*(1), 5-22.

Cohen, S., Schulz, M. S., Weiss, E., & Waldinger, R. J. (2012). Eye of the beholder: The individual and dyadic contributions of empathic accuracy and perceived empathic effort to relationship satisfaction. *Journal of Family Psychology*, *26*(2), 236-245.

Cole, M., & Morgan, K. (2011). Vegaphobia: Derogatory discourses of veganism and the reproduction of speciesism in UK national newspapers. *The British Journal of Sociology*, *62*(1), 134-153.

Coleman, L. M. (1986). Stigma. In *The dilemma of difference* (pp. 211-232). Springer, Boston, MA.

Corteen, K. (2002). Lesbian safety talk: Problematizing definitions and experiences of violence, sexuality and space. *Sexualities*, *5*(3), 259-280.

Cosslett, R. L. (2018, March 15). Anti-Welsh bigotry is rife. It's just as well we're a tough people. *The Guardian.* Retrieved from https://www.theguardian.com/commentisfree/2018/mar/15/anti-welsh-bigotry-eddie-jones-england-brexit

Costa, E., & Halpern, D. (2019). The behavioural science of online harm and manipulation, and what to do about it. *The Behavioural Insights Team.* Retrieved from https://www.bi.team/wp-content/uploads/2019/04/BIT_The-behavioural-science-of-online-harm-and-manipulation-and-what-to-do-about-it_Single.pdf

Crocker, J., & Major, B. (1989). Social stigma and self-esteem: The self-protective properties of stigma. *Psychological Review*, *96*(4), 608-630.

Culpan, D. (2015, August 25). ‘UK surveillance is worse than 1984’ says UN privacy chief. *Wired*. Retrieved from http://www.wired.co.uk/article/uk-digital-surveillance-joseph-cannataci

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science*, *48*(1), 28-46.

Davis, J. L., & Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. *Information, Communication & Society*, *17*(4), 476-485.

Dawson, S., Burnett, B., & McArdle, F. (2005, October). Watching learning from behind closed doors: The impact of surveillance on student online behaviour. In *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education* (pp. 1978-1985). Association for the Advancement of Computing in Education (AACE). Retrieved from http://eprints.qut.edu.au/2367/1/2367.pdf

De Laat, P. B. (2008). Online diaries: Reflections on trust, privacy, and exhibitionism. *Ethics and Information Technology*, *10*(1), 57-69.

de Zwart, M. D., Humphreys, S., & Dissel, B. V. (2014). Surveillance, big data and democracy: Lessons for Australia from the US and UK. *The University of New South Wales Law Journal, 37*, 713-747.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413-422.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Doosje, B., Ellemers, N., & Spears, R. (1995). Perceived intragroup variability as a function of group status and identification. *Journal of Experimental Social Psychology, 31*(5), 410-436.

Doyle, D. M., & Molix, L. (2014). How does stigma spoil relationships? Evidence that perceived discrimination harms romantic relationship quality through impaired self-image. *Journal of Applied Social Psychology*, *44*(9), 600-610.

Doyle, D. M., & Molix, L. (2016). Disparities in social health by sexual orientation and the etiologic role of self-reported discrimination. *Archives of Sexual Behavior*, *45*(6), 1317-1327.

Dubrofsky, R. E., & Wood, M. M. (2014). Posting racism and sexism: Authenticity, agency and self-reflexivity in social media. *Communication and Critical/Cultural Studies*, *11*(3), 282-287.

Dubrovsky, V. J., Kiesler, S., & Sethna, B. N. (1991). The equalization phenomenon: Status effects in computer-mediated and face-to-face decision-making groups. *Human-Computer Interaction*, *6*(2), 119-146.

Duhigg, C. (2012, February 16). How companies learn your secrets. *New York Times Magazine*. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&hp=&pagewanted=all

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and

MySpace. *AMCIS 2007 Proceedings*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.148.9388&rep=rep1&type=pdf

Ellis, D., Tucker, I., & Harper, D. (2013). The affective atmospheres of surveillance. *Theory & Psychology*, *23*(6), 716-731.

Emlet, C. A. (2016). Social, economic, and health disparities among LGBT older adults. *Generations*, *40*(2), 16-22.

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., ... & Sandvig, C. (2015). I always assumed that I wasn't really that close to [her]: Reasoning about Invisible Algorithms in News Feeds. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 153-162). ACM. Retrieved from https://www.ideals.illinois.edu/bitstream/handle/2142/55298/Algorithms_2014.pdf?sequence=2

Facebook (2015, February 11). Showing Relevance Scores for ads on Facebook. *Facebook.* Retrieved from https://www.facebook.com/business/news/relevance-score

Falk, G. (2001). *Stigma: How we treat outsiders*. Amherst, NY: Prometheus Books.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012, July). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. Retrieved from https://www.cs.ucy.ac.cy/courses/EPL682/papers/usable-1.pdf

Finkelstein, L. M., Ryan, K. M., & King, E. B. (2013). What do the young (old) people think of me? Content and accuracy of age-based metastereotypes. *European Journal of Work and Organizational Psychology*, *22*(6), 633-657.

Fischer, A. R., & Holz, K. B. (2007). Perceived discrimination and women's psychological distress: The roles of collective and personal self-esteem. *Journal of Counseling Psychology*, *54*(2), 154-164.

Foddy, M., Platow, M. J., & Yamagishi, T. (2009). Group-based trust in strangers: The role of stereotypes and expectations. *Psychological Science*, *20*(4), 419-422.

Fraser N (1995*)* From redistribution to recognition?: Dilemmas of justice in a 'postsocialist' age*. New Left Review, 212*, 68-93.

Friedland, G., & R. Sommer. 2010. Cybercasing the joint: On the privacy implication of geotagging. In *Proceedings of the 5th USENIX conference on hot topics in security.* Retrieved from https://www.usenix.org/legacy/events/hotsec10/tech/full_papers/Friedland.pdf

Frumin, A. (2013, June 26). 'Love is love': Americans rejoice over SCOTUS marriage decision. *MSNBC.* Retrieved from http://www.msnbc.com/hardball/love-love-americans-rejoice-over-scotus

Gao, G. (2015). What Americans think about NSA, national security and privacy. *Pew Research Center.* Retrieved from http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

Garrido, M. V. (2015). Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden. *Surveillance & Society*, *13*(2), 153-167.

Gay marriage legalised at midnight in England and Wales (2014, March 28). *BBC News*. Retrieved from https://www.bbc.co.uk/news/av/uk-26782081/gay-marriage-legalised-at-midnight-in-england-and-wales

Geiger, A. W. (2018, June 4). How Americans have viewed government surveillance and privacy since Snowdon leaks. *Pew Research Center.* Retrieved from https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261.

Gillmor, D. (2014, February 6). Get ready: The day we fight back against mass surveillance is coming. *The Guardian.* Retrieved from https://www.theguardian.com/commentisfree/2014/feb/06/nsa-fighting-back-against-surveillence-state

Gladfelter, O. (2018). Escaping the echo chamber: A study of how we engage with opposing political content. *The DataFace.* Retrieved from http://thedataface.com/2018/02/politics/echo-chambers#fnref-1

Glass, D. C., McKnight, J. D., & Valdimarsdottir, H. (1993). Depression, burnout, and perceptions of control in hospital nurses. *Journal of Consulting and Clinical Psychology*, *61*(1), 147-155.

Goette, L., Huffman, D., & Meier, S. (2006). The impact of group membership on cooperation and norm enforcement: Evidence using random assignment to real social groups. *American Economic Review*, *96*(2), 212-216.

Goffman, E. (1959). *The presentation of self in everyday life*. London, England: Harmondsworth.

Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity*. New York, NY: Touchstone.

Gómez, A., Seyle, D. C., Huici, C., & Swann Jr, W. B. (2009). Can self-verification strivings fully transcend the self–other barrier? Seeking verification of ingroup identities. *Journal of Personality and Social Psychology*, *97*(6), 1021-1044.

Graham, J. W. (2009). Missing data analysis: Making it work in the real world. *Annual Review of Psychology*, *60*, 549-576.

Graham, J., Nosek, B. A., & Haidt, J. (2012). The moral stereotypes of liberals and conservatives: Exaggeration of differences across the political spectrum. *PloS One*, *7*(12), 1-13.

Graham, S., & Wood, D. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy*, *23*(2), 227-248.

Greene, S. (2004). Social identity theory and party identification. *Social Science Quarterly*, *85*(1), 136-153.

Greenhow, C., & Robelia, B. (2009). Informal learning and identity formation in online social networks. *Learning, Media and Technology*, *34*(2), 119-140.

Greenwald, G. (2013, July 29). Major opinion shifts, in the US and Congress, on NSA surveillance and privacy. *The Guardian.* Retrieved from

https://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew

Griffin, J. M., Fuhrer, R., Stansfeld, S. A., & Marmot, M. (2002). The importance of low control at work and home on depression and anxiety: Do these effects vary by gender and social class? *Social Science & Medicine*, *54*(5), 783-798.

Han, G., & Harms, P. D. (2010). Team identification, trust and conflict: A mediation model. *International Journal of Conflict Management*, *21*(1), 20-43.

Harding, D. J. (2003). Jean Valjean's dilemma: The management of ex-convict identity in the search for employment. *Deviant Behavior*, *24*(6), 571-595.

Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737-3757.

Harmful gender stereotypes in adverts banned (2019, June 14). *BBC News.* Retrieved from https://www.bbc.co.uk/news/business-48628678

Haslam, S. A., Oakes, P. J., Reynolds, K. J., & Turner, J. C. (1999). Social identity salience and the emergence of stereotype consensus. *Personality and Social Psychology Bulletin*, *25*(7), 809-818.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Press.

Hirschler, C. A. (2011). “What pushed me over the edge was a deer hunter”: Being vegan in North America. *Society & Animals*, *19*(2), 156-174.

Hoare, J. (2010, January 4). What is the vilest piece of emotional blackmail on the internet? *Dirty Feed.* Retrieved from http://www.dirtyfeed.org/2010/01/emotional-blackmail/

Honneth A (1995) *The struggle for recognition: The moral grammar of social conflicts*, Cambridge: Polity Press.

Hopkins, N. (2011). Dual identities and their recognition: Minority group members' perspectives. *Political Psychology*, *32*(2), 251-270.

Hopkins, N., & Greenwood, R. M. (2013). Hijab, visibility and the performance of identity. *European Journal of Social Psychology*, *43*(5), 438-447.

Hopkins, N., Reicher, S., Harrison, K., Cassidy, C., Bull, R., & Levine, M. (2007). Helping to improve the group stereotype: On the strategic dimension of prosocial behavior. *Personality and Social Psychology Bulletin*, *33*(6), 776-788.

Hopkins, P., Botterill, K., Sanghera, G., & Arshad, R. (2017). Encountering misrecognition: Being mistaken for being Muslim. *Annals of the American Association of Geographers*, *107*(4), 934-948.

Howarth, C. (2002). So, you're from Brixton?' The struggle for recognition and esteem in a stigmatized community. *Ethnicities*, *2*(2), 237-260.

Humphrey, C. (2009). The mask and the face: Imagination and social life in Russian chat rooms and beyond. *Ethnos*, *74*(1), 31-50.

Hunt, E. (2016, June 29). How does Facebook suggest potential friends? Not location data – not now. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2016/jun/29/how-does-facebook-suggest-potential-friends-not-location-data-not-now

Hunter, J. (1990). Violence against lesbian and gay male youths. *Journal of Interpersonal Violence*, *5*(3), 295-300.

Hutton, V. E., Misajon, R., & Collins, F. E. (2013). Subjective wellbeing and 'felt' stigma when living with HIV. *Quality of Life Research*, *22*(1), 65-73.

Ilic, M., Reinecke, J., Bohner, G., Hans-Onno, R., Beblo, T., Driessen, M., ... & Corrigan, P. W. (2012). Protecting self-esteem from stigma: A test of different strategies for coping with the stigma of mental illness. *International Journal of Social Psychiatry*, *58*(3), 246-257.

Introna, L., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, *2*(2/3), 177-198.

Jacobsen, M. H, & Kristiansen, S. (2015). *The social thought of Erving Goffman.* Los Angeles, CA: SAGE Publications.

Jacobsen, P. L. (2015). Safety in numbers: More walkers and bicyclists, safer walking and bicycling. *Injury Prevention*, *21*(4), 271-275.

Jensen, J. M., Patel, P. C., & Messersmith, J. G. (2013). High-performance work systems and job control: Consequences for anxiety, role overload, and turnover intentions. *Journal of Management*, *39*(6), 1699-1724.

Jessen, F., Heun, R., Erb, M., Granath, D. O., Klose, U., Papassotiropoulos, A., & Grodd, W. (2000). The concreteness effect: Evidence for dual coding and context availability. *Brain and Language*, *74*(1), 103-112.

Jetten, J., Spears, R., & Postmes, T. (2004). Intergroup distinctiveness and differentiation: A meta-analytic integration. *Journal of Personality and Social Psychology*, *86*(6), 862-879.

Joiner, R., Brosnan, M., Duffield, J., Gavin, J., & Maras, P. (2007). The relationship between Internet identification, Internet anxiety and Internet use. *Computers in Human Behavior*, *23*(3), 1408-1420.

Jukes, K. (2016, May 17). A brief history of homophobia. *Rights Info.* Retrieved from https://rightsinfo.org/short-history-homophobia/

Kelly, A. E., & McKillop, K. J. (1996). Consequences of revealing personal secrets. *Psychological Bulletin*, *120*(3), 450-465.

Kelman, H. C. (2004). Reconciliation as identity change: A social-psychological perspective. In Y. Bar-Siman-Tov (Ed.), *From conflict resolution to reconciliation* (pp. 111-124). New York, NY: Oxford University Press.

Kennedy, H. (2006). Beyond anonymity, or future directions for internet identity research. *New Media & Society*, *8*(6), 859-876.

Kern, L. (2005). In place and at home in the city: Connecting privilege, safety and belonging for women in Toronto. *Gender, Place & Culture*, *12*(3), 357-377.

Khovanskaya, V., Baumer, E. P., Cosley, D., Voida, S., & Gay, G. (2013, April). Everybody knows what you're doing: A critical design approach to personal informatics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3403-3412). ACM. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.6511&rep=rep1&type=pdf

Klein, O., & Azzi, A. E. (2001). The strategic confirmation of meta-stereotypes: How group members attempt to tailor an out-group's representation of themselves. *British Journal of Social Psychology*, *40*(2), 279-293.

Klein, O., Spears, R., & Reicher, S. (2007). Social identity performance: Extending the strategic side of SIDE. *Personality and Social Psychology Review*, *11*(1), 28-45.

Klonoff, E. A., Landrine, H., & Campbell, R. (2000). Sexist discrimination may account for well-known gender differences in psychiatric symptoms. *Psychology of Women Quarterly*, *24*(1), 93-99.

Korshunov, P., & Ebrahimi, T. (2013). Using warping for privacy protection in video surveillance. In *Digital Signal Processing (DSP), 2013 18th International Conference* (pp. 1-6). IEEE. Retrieved from https://infoscience.epfl.ch/record/185947/files/dsp2013_korshunov_ebrahimi_warping.pdf

Koskela, H. (2000). 'The gaze without eyes': Video-surveillance and the changing nature of urban space. *Progress in Human Geography*, *24*(2), 243-265.

Koskela, H. (2004). Webcams, TV shows and mobile phones: Empowering exhibitionism. *Surveillance & Society*, *2*(2/3), 199-215.

Koskela, H., & M. Tuominen (2003). "Kakspiippunen juttu" – tutkimus helsinkiläisten suhtautumisesta kameravalvontaan. Research Reports of the Helsinki Urban Facts 2003:3. Retrieved from https://translate.google.co.uk/translate?hl=en&sl=fi&u=https://www.booky.fi/tuote/hille_koskela/kakspiippunen_juttu_tutkimus_helsinkilaisten_suhtautumisesta_kameravalvontaan/9789524731386&prev=search

Kozuch, E. (2017, December 15). #FlashbackFriday – today in 1973, the APA removed homosexuality from list of mental illnesses. *Human Rights*

Campaign. Retrieved from https://www.hrc.org/blog/flashbackfriday-today-in-1973-the-apa-removed-homosexuality-from-list-of-me

Laitinen, A. (2003. November 12). Social equality, recognition and preconditions of good life. *Social Inequality Today*. Retrieved from https://www.researchgate.net/profile/Arto_Laitinen/publication/251784959_Social_Equality_Recognition_and_Preconditions_of_Good_Life/links/53dbed470cf2a76fb667b0e6/Social-Equality-Recognition-and-Preconditions-of-Good-Life.pdf

Lanier, J. (2018, April). *How we need to remake the internet* [Video file]. Retrieved from https://www.ted.com/talks/jaron_lanier_how_we_need_to_remake_the_internet?language=en

Larson, R. (1989). Is feeling "in control" related to happiness in daily life? *Psychological Reports*, *64*(3), 775-784.

Lea, M., & Spears, R. (1991). Computer-mediated communication, de-individuation and group decision-making. *International Journal of Man-Machine Studies*, *34*(2), 283-301.

Leary, M. R., & Kowalski, R. M. (1990). Impression management: A literature review and two-component model. *Psychological Bulletin*, *107*(1), 34-47.

Lee, S. (2015, November 6). Julian Assange: 'Western civilization has produced a god, the god of mass surveillance'. *Huffington Post*. Retrieved from https://www.huffingtonpost.com/seungyoon-lee/julian-assange_1_b_7560710.html

Livingstone, A. G., Fernández Rodríguez, L., & Rothers, A. (in press). "They just don't understand us": The role of felt understanding in intergroup

relations. *Journal of Personality and Social Psychology*. Advance online publication retrieved from http://dx.doi.org/10.1037/pspi0000221

Lindquist, A. (2013). *Beyond hippies and rabbit food: The social effects of vegetarianism and veganism.* (Doctoral dissertation or Master's thesis, University of Puget Sound, Tacoma, Washington, USA). Retrieved from https://soundideas.pugetsound.edu/cgi/viewcontent.cgi?referer=https://scholar.google.co.uk/&httpsredir=1&article=1008&context=honors_program_theses

Lonsdale, A. J., & North, A. C. (2009). Musical taste and ingroup favouritism. *Group Processes & Intergroup Relations*, *12*(3), 319-327.

Luhtanen, R. K. (2002). Identity, stigma management, and well-being: A comparison of lesbians/bisexual women and gay/bisexual men. *Journal of Lesbian Studies*, *7*(1), 85-100.

Luhtanen, R., & Crocker, J. (1992). A collective self-esteem scale: Self-evaluation of one's social identity. *Personality and Social Psychology Bulletin, 18*, 302-318.

Lun, J., Kesebir, S., & Oishi, S. (2008). On feeling understood and feeling well: The role of interdependence. *Journal of Research in Personality*, *42*(6), 1623-1628.

Lupton, D. (2014). *Digital sociology*. New York, NY: Routledge.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London, England: Routledge.

Maass, P. (2015, May 28). Inside NSA, officials privately criticize 'collect it all' surveillance. *The Intercept.* Retrieved from

https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/

MacInnis, C. C., & Hodson, G. (2015). It ain't easy eating greens: Evidence of bias toward vegetarians and vegans from both source and target. *Group Processes & Intergroup Relations*, *20*(6), 721-744.

Major, B., & Schmader, T. (1998). Coping with stigma through psychological disengagement. In J. K. Swim & C. Stangor (Eds.), *Prejudice: The target's perspective* (pp. 219-241). San Diego, CA: Academic Press.

Major, B., Kaiser, C. R., & McCoy, S. K. (2003). It's not my fault: When and why attributions to prejudice protect self-esteem. *Personality and Social Psychology Bulletin*, *29*(6), 772-781.

Major, B., Spencer, S., Schmader, T., Wolfe, C., & Crocker, J. (1998). Coping with negative stereotypes about intellectual performance: The role of psychological disengagement. *Personality and Social Psychology Bulletin*, *24*(1), 34-50.

Mamonov, S., & Koufaris, M. (2016). The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy and Security*, *12*(2), 56-67.

Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*, *11*(1/2), 18-34.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*(3), 5-21.

Marthews, A., & Tucker, C. E. (2017, February 17). Government surveillance and internet search behavior. *SSRN.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378-393.

Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114-133.

Mason, C. L., & Magnet, S. (2012). Surveillance studies and violence against women. S*urveillance & Society*, *10*(2), 105-118.

McDonald, A., & Cranor, L. F. (2010, August 16). Beliefs and behaviors: Internet users' understanding of behavioral advertising. *TPRC.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092

McGrath, J. (2004). *Loving Big Brother: Performance, privacy and surveillance space.* London, England: Routledge.

McLean, K. (2008). Silences and stereotypes: The impact of (mis) constructions of bisexuality on Australian bisexual men and women. *Gay & Lesbian Issues and Psychology Review*, *4*(3), 158-165.

McLeish, K. N., & Oxoby, R. J. (2007). Identity, cooperation, and punishment. *Institute for the Study of Labor.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=961379

Meisenbach, R. J. (2010). Stigma management communication: A theory and agenda for applied research on how individuals manage moments of stigmatized identity. *Journal of Applied Communication Research*, *38*(3), 268-292.

Melvin, J. (2012, February 1). Google defends change to privacy policies. *Reuters.* Retrieved from https://uk.reuters.com/article/us-google-privacy-policy/google-defends-change-to-privacy-policies-idUKTRE80U1UL20120201

Miller (2013). What is the relationship between identities that people construct, express and consume online and those offline? In *Future identities: Changing identities in the IK – the next 10 years.* Oxford Internet Institute, commissioned by the UK Government's Foresight Project: Government office for science. Retrieved from https://discovery.ucl.ac.uk/id/eprint/1394763/1/13-504-relationship-between-identities-online-and-offline%20(1).pdf

Miller, C. T., & Kaiser, C. R. (2001). A theoretical perspective on coping with stigma. *Journal of Social Issues*, *57*(1), 73-92.

Möllers, N., & Hälterlein, J. (2013). Privacy issues in public discourse: The case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1-2), 57-70.

Morelli, S. A., Torre, J. B., & Eisenberger, N. I. (2014). The neural bases of feeling understood and not understood. *Social Cognitive and Affective Neuroscience*, *9*(12), 1890-1896.

Mummendey, A., & Schreiber, H. J. (1984). 'Different 'just means 'better': Some obvious and some hidden pathways to in-group favouritism. *British Journal of Social Psychology*, *23*(4), 363-367.

Munro, G. D. (2010). The scientific impotence excuse: Discounting belief-threatening scientific abstracts. *Journal of Applied Social Psychology*, *40*(3), 579-600.

Murphy, M. H. (2017). Algorithmic surveillance: The collection conundrum. *International Review of Law, Computers & Technology*, *31*(2), 225-242.

Murray, S. L., Holmes, J. G., Bellavia, G., Griffin, D. W., & Dolderman, D. (2002). Kindred spirits? The benefits of egocentrism in close relationships. *Journal of Personality and Social Psychology*, *82*(4), 563-581.

Nagda, B. A., Gurin, P., Sorensen, N., & Zúñiga, X. (2009). Evaluating intergroup dialogue: Engaging diversity for personal and social responsibility. *Diversity & Democracy*, *12*(1), 1-7.

Neville, F., & Reicher, S. (2011). The experience of collective participation: Shared identity, relatedness and emotionality. *Contemporary Social Science*, *6*(3), 377-396.

Newheiser, A. K., & Barreto, M. (2014). Hidden costs of hiding stigma: Ironic interpersonal consequences of concealing a stigmatized identity in social interactions. *Journal of Experimental Social Psychology*, *52*, 58-70.

Newton, C. (2019, March 8). Facebook's pivot to privacy has huge implications if it's real. *The Verge.* Retrieved from https://www.theverge.com/interface/2019/3/6/18253922/facebook-privacy-meaning-implications-mark-zuckerberg-pivot-analysis-interface-casey-newton

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119-158.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

O'Donnell, A. T., Ryan, M. K., & Jetten, J. (2012). The hidden costs of surveillance for performance and helping behaviour. *Group Processes & Intergroup Relations*, *16*(2), 246-256.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy.* London, England: Penguin UK.

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

O'Donnell, A. T., Jetten, J., & Ryan, M. K. (2010a). Who is watching over you? The role of shared identity in perceptions of surveillance. *European Journal of Social Psychology*, *40*(1), 135-147.

O'Donnell, A. T., Jetten, J., & Ryan, M. K. (2010b). Watching over your own: How surveillance moderates the impact of shared identity on perceptions of leaders and follower behaviour. *European Journal of Social Psychology*, *40*(6), 1046-1061.

Oishi, S., Krochik, M., & Akimoto, S. (2010). Felt understanding as a bridge between close relationships and subjective well-being: Antecedents and consequences across individuals and cultures. *Social and Personality Psychology Compass*, *4*(6), 403-416.

OneTrust. (n.d.). What's the cookie law all about? *OneTrust.* Retrieved from https://www.cookielaw.org/faq/

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., ... & Myllymäki, P. (2012). Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 41-50). ACM. Retrieved from https://www.researchgate.net/profile/Niklas_Vainio/publication/262324308_Long-term_effects_of_ubiquitous_surveillance_in_the_home/links/5a04174caca272b06ca79169/Long-term-effects-of-ubiquitous-surveillance-in-the-home.pdf

Oyserman, D. (2004). Self-concept and identity. In M. B. Brewer & M. E Hewstone (Eds.) *Self and social identity* (pp. 499-517). Malden, MA: Blackwell Pub.

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, *65*(6), 526-536.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. New York, NY: Penguin Group.

Park, K. (2002). Stigma management among the voluntarily childless. *Sociological Perspectives*, *45*(1), 21-45.

Patel, T. G. (2012). Surveillance, suspicion and stigma: Brown bodies in a terror-panic climate. *Surveillance & Society*, *10*(3/4), 215-234.

Pavone, V., & Esposti, S. D. (2010). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, *21*(5), 556-572.

Pehrson, S., Stevenson, C., Muldoon, O. T., & Reicher, S. (2014). Is everyone Irish on St Patrick's Day? Divergent expectations and experiences of collective self-objectification at a multicultural parade. *British Journal of Social Psychology*, *53*(2), 249-264.

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, *31*(1), 117-182.

Pham, V. H., Tran, D. P., & Hoang, V. D. (2019). Personal identification based on deep learning technique using facial images for intelligent surveillance systems. *International Journal of Machine Learning and Computing*, *9*(4), 465-470.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.

Postmes, T., & Spears, R. (2002). Behavior online: Does anonymous computer communication reduce gender inequality? *Personality and Social Psychology Bulletin*, *28*(8), 1073-1083.

Preston, A. (August 3, 2014). The death of privacy. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

Quarter of children under six have a smartphone, study finds (2018, April 8). *The Independent.* Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/children-smartphone-ideal-age-social-media-snapchat-youtube-a8294701.html

Radical Preachy Vegan. (2015, September 12). I'm vegan but not gluten free. [Post on Reddit]. *Reddit.* Retrieved from

https://www.reddit.com/r/vegan/comments/3koixt/im_vegan_but_not_gluten_free/

Reicher, S. D., Spears, R., & Postmes, T. (1995). A social identity model of deindividuation phenomena. *European Review of Social Psychology*, *6*(1), 161–198.

Reis, H. T., Lemay Jr, E. P., & Finkenauer, C. (2017). Toward understanding understanding: The importance of feeling understood in relationships. *Social and Personality Psychology Compass*, *11*(3), 1-22.

Renger, D., Renger, S., Miché, M., & Simon, B. (2017). A social recognition approach to autonomy: The role of equality-based respect. *Personality and Social Psychology Bulletin*, *43*(4), 479-492.

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000-1011.

Rossman, K., Salamanca, P., & Macapagal, K. (2017). "The doctor said I didn't look gay": Young adults' experiences of disclosure and non-disclosure of LGBTQ identity to healthcare providers. *Journal of Homosexuality*, *64*(10), 1390-1410.

Rothgerber, H. (2012). Real men don't eat (vegetable) quiche: Masculinity and the justification of meat consumption. *Psychology of Men & Masculinity*, *14*(4), 1-13.

Rydell, R. J., McConnell, A. R., & Beilock, S. L. (2009). Multiple social identities and stereotype threat: Imbalance, accessibility, and working memory. *Journal of Personality and Social Psychology*, *96*(5), 949-966.

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2015). Can an Algorithm be Unethical? In *65th annual meeting of the International Communication Association.* Retrieved from www-personal.umich.edu/~csandvig/research/ICA2015--CananAlgorithmbeUnethical.pdf

Saroglou, V., Yzerbyt, V., & Kaschten, C. (2011). Meta-stereotypes of groups with opposite religious views: Believers and non-believers. *Journal of Community & Applied Social Psychology*, *21*(6), 484-498.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* New York, NY: W. W. Norton & Company.

Schneier, B. (2016, February 3). Security vs. surveillance. *Schneier on Security.* Retrieved from https://www.schneier.com/blog/archives/2016/02/security_vs_sur.html

Shechtman, Z., & Bar-El, O. (1994). Group guidance and group counseling to foster social acceptability and self-esteem in adolescence. *Journal for Specialists in Group Work*, *19*(4), 188-196.

Shelton, M., Rainie, L., Madden, M., Anderson, M., Duggan, M., Perrin, A., & Page, D. (2015). Americans' privacy strategies post-Snowden. *Pew Research Center Internet, Science, and Technology Project*. Retrieved from http://www.pewinternet.org/2015/03/16/americansprivacy-strategies-post-snowden/

Shih, M. (2004). Positive stigma: Examining resilience and empowerment in overcoming stigma. *The ANNALS of the American Academy of Political and Social Science*, *591*(1), 175-185.

Sigelman, L., & Tuch, S. A. (1997). Metastereotypes: Blacks' perceptions of Whites' stereotypes of Blacks. *The Public Opinion Quarterly*, *61*(1), 87-101.

Simon, B., & Grabow, H. (2014). To be respected and to respect: The challenge of mutual respect in intergroup relations. *British Journal of Social Psychology*, *53*(1), 39-53.

Simon, B., & Oakes, P. (2006). Beyond dependence: An identity approach to social power and domination. *Human Relations*, *59*(1), 105-139.

Skeggs, B. (1999). Matter out of place: Visibility and sexualities in leisure spaces. *Leisure Studies*, *18*(3), 213-232.

Skillinger, T. (2016). Petition to Repeal the New Surveillance Laws (Investigatory Powers Act). Retrieved from https://petition.parliament.uk/archived/petitions/173199

Smith, D. (2015, January 25). Google chairman: 'The internet will disappear'. *Business Insider.* Retrieved from https://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1?r=US&IR=T

Snow, D. A., & Anderson, L. (1987). Identity work among the homeless: The verbal construction and avowal of personal identities. *American Journal of Sociology*, *92*(6), 1336-1371.

Spalek, B., & Lambert, B. (2007). Muslim communities under surveillance. *Criminal Justice Matters, 68*(1), 12-13.

Spears, R., & Lea, M. (1994). Panacea or panopticon? The hidden power of computer-mediated communication. *Communication Research*, *21*(4), 427–459.

Spears, R., Lea, M., Corneliussen, R. A., Postmes, T., & Haar, W. T. (2002). Computer-mediated communication as a channel for social resistance: The strategic side of SIDE. *Small Group Research*, *33*(5), 555-574.

Special report welsh men are “most stupid”. (1999, July 12). *British Broadcasting Corporation.* Retrieved from http://news.bbc.co.uk/1/hi/special_report/392450.stm

Spector, P. E., Cooper, C. L., Sanchez, J. I., O'Driscoll, M., Sparks, K., Bernin, P., ... & Miller, K. (2002). Locus of control and well-being at work: How generalizable are western findings? *Academy of Management Journal*, *45*(2), 453-466.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38-47). ACM. Retrieved from http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf

Starr, A., Fernandez, L. A., Amster, R., Wood, L. J., & Caro, M. J. (2008). The impacts of state surveillance on political assembly and association: A socio-legal analysis. *Qualitative Sociology*, *31*(3), 251-270.

Statistica (n.d.) *Number of monthly active WhatsApp users worldwide from April 2013 to January 2017 (in millions)*. Retrieved from www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users

Steele, C. M., Spencer, S. J., & Aronson, J. (2002). Contending with group image: The psychology of stereotype and social identity threat. In M.

Zanna (Ed.) *Advances in experimental social psychology* (Vol. 34, pp. 379-440). San Diego, CA: Academic Press.

Steeves, V., & Bailey, J. (2016). Living in the mirror: Understanding young women's experiences with online social networking. *Ottawa Faculty of Law Working Paper*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2714706

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296-311.

Stuart, A., & Levine, M. (2017). Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology*, *47*(6), 694-707.

Stuart, A., Bandara, A. K. & Levine, M. (2019). The psychology of privacy in the digital age. *Social and Personality Psychology Compass, 13*(11), 1-14.

Subašić, E., Reynolds, K. J., Turner, J. C., Veenstra, K. E., & Haslam, S. A. (2011). Leadership, power and the use of surveillance: Implications of shared social identity for leaders' capacity to influence. *The Leadership Quarterly*, *22*(1), 170-181.

Summers, C. A., Smith, R. W., & Reczek, R. W. (2016). An audience of one: Behaviorally targeted ads as implied social labels. *Journal of Consumer Research*, *43*(1), 156-178.

Swann Jr, W. B., & Read, S. J. (1981). Self-verification processes: How we sustain our self-conceptions. *Journal of Experimental Social Psychology*, *17*(4), 351-372.

Swann Jr, W. B., Rentfrow, P. J., & Guinn, J. (2003). Self-verification: The search for coherence. In M. Leary & J. Tangney (Eds.) *Handbook of self and identity* (pp. 367-383). New York, NY: Guilford press.

Sylvestre, J. (2009). Veganism and punk – a recipe for resistance: Symbolic discourse and meaningful practice. *Ottawa Journal of Religion.* Retrieved from https://ruor.uottawa.ca/bitstream/10393/26045/1/Sylvestre_Julie_2009.pdf

Tajfel, H. (1981). *Human groups and social categories: Studies in social psychology*. Cambridge. England: Cambridge University Press.

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. Austin & S. Worchel (Eds.), *The social psychology of intergroup relations* (pp. 33-47). Monterey. CA: Brooks/Cole.

Tajfel, H., Billig, M. G., Bundy, R. P., & Flament, C. (1971). Social categorization and intergroup behaviour. *European Journal of Social Psychology*, *1*(2), 149-178.

Tanis, M., & Postmes, T. (2005). A social identity approach to trust: Interpersonal perception, group membership and trusting behaviour. *European Journal of Social Psychology*, *35*(3), 413-424.

Taylor C (1994) The politics of recognition. In: Gutmann A (ed) *Multiculturalism: Examining the politics of recognition.* Princeton, NJ: Princeton University Press.

Taylor, Y. (2007). 'If your face doesn't fit…': The misrecognition of working-class lesbians in scene space. *Leisure Studies*, *26*(2), 161-178.

Tech Crunch (2016, August 25). *WhatsApp to share user data with Facebook for ad-targeting – here's how to opt out*. Retrieved from www.techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out

Tene, O., & Polonetsky, J. (2014). A theory of creepy: Technology, privacy and shifting social norms. *Yale Journal of Law & Technology, 16*(1), 58-102.

The Happy Pear. (n.d.). The difference between a whole food plant-based diet and a vegan diet. Retrieved from https://thehappypear.ie/the-difference-between-whole-food-plant-based-and-vegan/

The Independent. (n.d.). *Cookie Policy*. Retrieved from https://www.independent.co.uk/service/cookie-policy-a6184186.html

Toma, C. L., & Hancock, J. T. (2013). Self-affirmation underlies Facebook use. *Personality and Social Psychology Bulletin*, *39*(3), 321-331.

Travis, A. (2016, November 29). 'Snoopers charter' becomes law, extending UK state surveillance. *The Guardian*. Retrieved from https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20-36.

Turner, J. C., Brown, R. J., & Tajfel, H. (1979). Social comparison and group interest in ingroup favouritism. *European Journal of Social Psychology*, *9*(2), 187-204.

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). *Rediscovering the social group: A self-categorization theory*. Oxford. England: Basil Blackwell.

Twenge, J. M., & Crocker, J. (2002). Race and self-esteem: Meta-analyses comparing Whites, Blacks, Hispanics, Asians, and American Indians and comment on Gray-Little and Hafdahl (2000). *Psychological Bulletin, 128*(3), 371-408.

Unidrain. (2018). Why does Unidrain use cookies? Retrieved from https://www.unidrain.com/omunidrainfolderen/cookies-we-use-cookies-to-improve-the-user-experience/

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *proceedings of the eighth symposium on usable privacy and security* (p. 1-15). ACM. Retrieved from https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab12007.pdf

Vaidhyanathan, S. (2018). *Anti-social media: How Facebook disconnects us and undermines democracy.* New York, NY: Oxford University Press.

van Leeuwen, E., & Täuber, S. (2012). Outgroup helping as a tool to communicate ingroup warmth. *Personality and Social Psychology Bulletin*, *38*(6), 772-783.

Vandenberg, R. J. (2006). Statistical and methodological myths and urban legends: Where, pray tell, did they get this idea? *Organization Research Methods, 9*(2), 194-201.

Vega, T. (2010, September 20). Code that tracks users' browsing prompts lawsuits. *New York Times.* Retrieved from http://www.nytimes.com/2010/09/21/technology/21cookie.html.

Verkuyten, M. (2006). Multicultural recognition and ethnic minority rights: A social identity perspective. *European Review of Social Psychology*, *17*(1), 148-184.

Verme, P. (2009). Happiness, freedom and control. *Journal of Economic Behavior & Organization*, *71*(2), 146-161.

Vorauer, J. D., Main, K. J., & O'Connell, G. B. (1998). How do individuals expect to be viewed by members of lower status groups? Content and implications of meta-stereotypes. *Journal of Personality and Social Psychology*, *75*(4), 917-937.

Vote leave's targeted Brexit ads released by Facebook (2018, July 26). *BBC News*. Retrieved from https://www.bbc.co.uk/news/uk-politics-44966969

Walby, K., & Monaghan, J. (2011). Private eyes and public order: Policing and surveillance in the suppression of animal rights activists in Canada. *Social Movement Studies*, *10*(01), 21-37.

Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., & Sadeh, N. (2014, April). A field trial of privacy nudges for Facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2367-2376). ACM. Retrieved from https://dl.acm.org/doi/abs/10.1145/2556288.2557413

Welinder, Y. (2012). A face tells more than a thousand posts: Developing face recognition privacy in social networks. *Harvard Journal of Law & Technology*, *26*, 165-239.

Wesch, M. (2009). Youtube and you: Experiences of self-awareness in the context collapse of the recording webcam. *Explorations in Media Ecology*, *8*(2), 19-34.

West, S. M. (2017). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20-41.

Westin, A. F. (1967). *Privacy and freedom.* New York, NY: Atheneum Press.

Whistle-blower: Brexit vote part of Facebook data scandal (2018, March 27). *Aljazeera.* Retrieved from https://www.aljazeera.com/news/2018/03/whistle-blower-brexit-vote-part-facebook-data-scandal-180327174002761.html

Wilkins, D. J., Livingstone, A.G., & Levine, M. (2017). *Reconsidering slacktivism: Online collective action, perceived efficacy and activism experience combine to affect further participation* [Unpublished manuscript]. Psychology Department, University of Exeter, England.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, *18*(4), 326-348.

Xu, H., & Teo, H. H. (2004). Alleviating consumers' privacy concerns in location-based services: A psychological control perspective. *ICIS 2004 Proceedings*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.359.6132&rep=rep1&type=pdf

Yougov (2013, August). YouGov/The Sunday Times survey results. Retrieved from

https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/9ytf2ekflo/YG-Archive-Pol-Sunday-Times-results-230813.pdf

Zeng, F., Huang, L., & Dou, W. (2009). Social factors in user perceptions and responses to advertising in online social networking communities. *Journal of Interactive Advertising*, *10*(1), 1-13.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* London, England: Profile Books Ltd.

Zurn, C. F. (2003). Identity or status? Struggles over 'recognition' in Fraser, Honneth, and Taylor. *Constellations*, 10(4), 519-537.

APPENDICES

Appendix A: Study 1 manipulation article

Page 1 (consistent between studies)

Technology

Our digital footprint: are algorithms any good at tracking us online?

We are in the age of data surveillance: so what does this mean for us?

Got a smartphone? A computer? Laptop or tablet? Then it's official; algorithmic surveillance is part of your everyday life (and for the record, it's not going anywhere). By buying a book on Amazon, liking a page on Facebook, or even making a casual Google search, we leave a digital trail. Organisations like Amazon, Google, Facebook, and also the government harvest our digital footprints to make conclusions and predictions about who we are. From your online purchases, Amazon may label you a Sci-Fi fan and subsequently suggest you buy the genre's latest paperback. The government on the other hand may use your social media activity to predict how likely it is that you'll engage in some radical or activist behaviour. Whatever the source or the motive, algorithms are continuously scrutinising our online behaviour.

You may be thinking 'so what if Amazon knows that I've pre-ordered *Rogue One: A Star Wars Story* on Blu-Ray?'. Granted, at first glance algorithmic surveillance appears to have fairly superficial information about us. However, Professor Flynn Brigstock from Columbia University speaks to *Wired* UK to describe the true reach of algorithmic surveillance: 'algorithms have their fingers in a lot of pies' explains Brigstock, 'they gather data on what you do on *multiple* websites, and piece this together to create a profile about who you are...this profile is then used to make predictions about our future; the aim is to know our thoughts, plans, and desires before we do'. For example, algorithms may suggest we apply for a loan, before we realise we need one. Additionally, algorithms can predict that we are likely to become sick, before we start feeling ill. All in all, algorithms are designed to know us better than we know ourselves.

'the aim is to know our thoughts, plans, and desires before we do'

The average internet user is affected by this in many significant ways. Professor Brigstock continues: 'at a consumer level, algorithmic surveillance can hike up the price of our purchases. If you are using an Apple product to buy something online, the prices may be higher because they assume you have a higher income than someone using a Windows computer'. But it doesn't end at our finances; their predictions can get a lot more personal. Infamously, an American teenage girl was sent vouchers for baby products by the store Target (the equivalent to *ASDA* in the UK). Furious, her

father complained to Target at the inappropriateness of these promotions, until his teenage daughter later confessed that she was indeed pregnant. Target knew of her pregnancy before her own father due to her purchasing behaviour at their store. But of course, Brigstock explains that our data doesn't just fall into the hands of corporations like Target. In 2012, a British man was refused entry into the USA for a holiday due to a (later discovered innocent) Tweet. 'Our digital trace can have consequences for how our government at home and those abroad treat us. You may think your activity on social media is harmless, but this activity is harvested by algorithms and fed back to intelligence agencies. Based on this data, governments can determine the limits of our freedoms, such as our admittance on a long haul flight.' Therefore, the repercussions of algorithmic surveillance for the average internet user should not be underestimated.

But how accurate are these algorithms? Working with major organisations, Professor Brigstock has been analysing their efficacy for over a decade, and the prognosis is poor: 'algorithms are not sophisticated enough to piece together the many digital traces we leave online'. In fact, Brigstock analysed thousands of profiles generated from algorithmic surveillance and found that on average, only 19% of profiles were accurate:

'algorithms are not sophisticated enough to piece together the many digital traces we leave online'

'people were misrecognised on the vast majority of occasions in terms of gender, occupation, nationality, romantic status, age, and sexuality'. For example, internet users would often have an incorrect sexual preference attached to their profile. 'many of us have had a friend change our gender or sexual orientation on Facebook; yet algorithms will routinely fail to discount this erroneous information, and add an incorrect gender or sexuality to your profile'. This is often despite contradictory data elsewhere, such as any registration or membership forms you may have completed online.

All in all, Silicon Valley's promise of the crystal ball algorithm has not exactly been fulfilled. While the internet is a data free-for-all, those who endeavour to make sense of it are not doing a particularly good job. Indeed, they attempted to design algorithms which know us better than we know ourselves, yet the flaws of algorithms suggest that our own predictions should still be trusted over any algorithm when it comes to forecasting our own future. Whether this is good or bad news should ultimately be decided by those who generate the data in the first place; the internet users themselves.

'people were misrecognised on the vast majority of occasions'

father complained to Target at the inappropriateness of these promotions, until his teenage daughter later confessed that she was indeed pregnant. Target knew of her pregnancy before her own father due to her purchasing behaviour at their store. But of course, Brigstock explains that our data doesn't just fall into the hands of corporations like Target. In 2012, a British man was refused entry into the USA for a holiday due to a (later discovered innocent) Tweet. 'Our digital trace can have consequences for how our government at home and those abroad treat us. You may think your activity on social media is harmless, but this activity is harvested by algorithms and fed back to intelligence agencies. Based on this data, governments can determine the limits of our freedoms, such as our admittance on a long haul flight.' Therefore, the repercussions of algorithmic surveillance for the average internet user should not be underestimated.

But how accurate are these algorithms? Working with major organisations, Professor Brigstock has been analysing their efficacy for over a decade, and the prognosis is mixed: 'algorithms can occasionally piece together the many digital traces we leave online'. Brigstock analysed thousands of profiles generated from algorithmic surveillance and found that on average, 50% of profiles were accurate: 'on half of the occasions people were misrecognised in terms of gender, occupation, nationality, romantic status, age, and sexuality'. For example, internet users would sometimes have an incorrect sexual preference attached to their profile. 'many of us have had a friend change our gender or sexual orientation on Facebook; algorithms will occasionally fail to discount this erroneous information, and add an incorrect gender or sexuality to your profile'. However, for accurate profiles, algorithms use contradictory data elsewhere on the internet, such as registration or membership forms completed online, to indicate the user's true characteristics.

'algorithms can occasionally piece together the many digital traces we leave online'.

All in all, Silicon Valley's promise of the crystal ball algorithm has partially been fulfilled. It's clear the internet is a data free-for-all, but for those who endeavour to make sense of it, it continues to be an ongoing struggle where the rewards are occasionally worth the effort. While they may have designed algorithms to know us better than we know ourselves, it seems that despite their valuable insight at times, an algorithm's predictions can't yet be trusted over our own. Whether this is good or bad news should ultimately be decided by those who generate the data in the first place; the internet users themselves.

'on half of the occasions people were misrecognised'

father complained to Target at the inappropriateness of these promotions, until his teenage daughter later confessed that she was indeed pregnant. Target knew of her pregnancy before her own father due to her purchasing behaviour at their store. But of course, Brigstock explains that our data doesn't just fall into the hands of corporations like Target. In 2012, a British man was refused entry into the USA for a holiday due to a (later discovered innocent) Tweet. 'Our digital trace can have consequences for how our government at home and those abroad treat us. You may think your activity on social media is harmless, but this activity is harvested by algorithms and fed back to intelligence agencies. Based on this data, governments can determine the limits of our freedoms, such as our admittance on a long haul flight.' Therefore, the repercussions of algorithmic surveillance for the average internet user should not be underestimated.

But how accurate are these algorithms? Working with major organisations, Professor Brigstock has been analysing their efficacy for over a decade, and the prognosis is impressive: 'algorithms have the ability to piece together the many digital traces we leave online'. In fact, Brigstock analysed thousands of profiles generated from algorithmic surveillance and found that on average, 81% of profiles were accurate: 'in very few cases were people misrecognised in terms of gender, occupation, nationality, romantic status, age, and sexuality'. For example, internet users would routinely have the correct sexual preference attached to their profile. 'despite many of us experiencing a friend change our gender or sexual orientation on Facebook; algorithms will consistently discount this erroneous information, and instead add your correct gender or sexuality to your profile'. Algorithms often achieve this by using contradictory data elsewhere, such as any registration or membership forms you may have completed online.

'algorithms have the ability to piece together the many digital traces we leave online'

All in all, Silicon Valley's promise of the crystal ball algorithm has seemingly been fulfilled. While the internet is a data free-for-all, those who endeavour to make sense of it are doing a particularly good job. Indeed, algorithms have ultimately been designed to, and now appear to succeed at, knowing us better than we know ourselves. Whether this is good or bad news should ultimately Be decided by those who generate the data in the first place; the internet users themselves.

'in very few cases were people misrecognised'

Appendix B: Study 1 full list of measures

Manipulation check:

In my view, algorithmic surveillance is…

1. … accurate in identifying people
2. … usually unable to predict what internet users will do
3. … usually unable to identify people's characteristics
4. … able to predict behaviour accurately
5. …able to access many aspects of people's lives
6. …limited in what types of information it can gather on people

Feelings towards surveillance:

Algorithmic surveillance (i.e. the tracking and analysis of my behaviour and personal information online) makes me feel:

1. Worried/Calm
2. Anxious/Relaxed
3. Angry/Happy
4. Annoyed/Pleased
5. Disinterested/engaged
6. Unsafe/Safe
7. Frightened/Reassured
8. Uncomfortable/Comfortable

9. Repressed/Free
10. Powerless/In control
11. Visible/Invisible
12. Identifiable/Anonymous
13. Observed/Unobserved
14. Known/Unknown
15. Misinterpreted/Understood
16. Judged/Not judged

Privacy concern:

1. Internet surveillance is an invasion of privacy
2. Internet users have a right to use the internet without being surveilled
3. When online, it is fair to exchange your privacy for the use of a website
4. You shouldn't expect privacy when using the internet

Safety concern:

1. Algorithmic surveillance makes me feel less safe using the internet
2. If you have nothing to hide, then algorithmic surveillance shouldn't concern you
3. There is little to suggest that surveillance online makes society safer
4. Algorithmic surveillance can help prevent crime

Consumer opportunity:

1. Algorithmic surveillance can bias what we are exposed to online
2. Algorithmic surveillance does not benefit consumers

3. Targeted adverts online resulting from algorithmic surveillance are often useful
4. Algorithmic surveillance can help consumers save money

Behaviour change intentions:

1. I feel concerned about what I do online because of surveillance
2. I have or will censor what I do online because of surveillance
3. Algorithmic surveillance would not make me change what I do online
4. Algorithmic surveillance doesn't make me concerned about what I do online

Surveiller motive/trust:

1. If organisations use algorithmic surveillance, they do not respect internet users
2. Organisations that use algorithmic surveillance do not care about internet users
3. Algorithmic surveillance is used to help internet users
4. Organisations that use algorithmic surveillance have internet users' best interests at heart

Perceived value of surveillance:

1. Algorithmic surveillance shouldn't be used to make decisions about people's lives
2. Algorithmic surveillance is a useful way to sort and manage people's data

Recognition:

Accuracy:

1. Algorithmic surveillance can accurately portray everything about me
2. It is unlikely that algorithmic surveillance has built an accurate picture of who I am

Discrimination:

3. Internet users could be treated unfairly because of algorithmic surveillance
4. Algorithmic surveillance does not discriminate against me
5. I could be treated unfairly as a result of algorithmic surveillance
6. Algorithmic surveillance by its nature is always unbiased

Scrutiny:

7. The use of algorithmic surveillance makes me feel analysed
8. The use of algorithmic surveillance makes me feel judged

Distinctiveness:

9. Algorithmic surveillance is unable to recognise the ways that I am different from others
10. Algorithmic surveillance can accurately distinguish me from others

Depth:

11. Someone using algorithmic surveillance could know me better than I know myself

12. Someone using algorithmic surveillance would have no idea who I truly am

Perceived online control (adapted from Reid and Ware's (1974) three-factor internal-external scale):

Self-control:

1. I often give in to pressure to disclose my personal information online
2. I always feel in control of my personal information online
3. Controlling who has your online data is always possible
4. I often give in to pressure to sign up to things online

Social control:

5. People will always be tracked online, no matter how much we try and stop it
6. The flow of my data online is entirely governed by others
7. If enough people tried to stop algorithmic surveillance, it could be stopped
8. Where my data goes online is mostly under my control

Fatalism:

9. The harder you try, the more likely you are to gain control over your data
10. If your data leaks online, it is often due to a mistake you have made
11. There is no point trying to control what happens to your data
12. Whether you want it to or not, your data can accidentally leak to areas of the internet

Free will (adapted from Nadelhoffer et al.'s (2014) The Free Will Inventory):

Free will:

1. I always have free will
2. If I click on a link/website, it is because I want to and not because I feel influenced to
3. Nothing influences my behaviour online
4. I have free will even when my choices are limited by external forces
5. Only I can know the reasons behind my actions
6. I am not very predictable online

Determinism:

7. What I do is completely determined by prior events
8. If an algorithm knows what I have done up until this point, it could calculate everything that I would do in the future
9. My decisions and actions are dictated by my experiences and/or biology
10. If you know which websites I have previously visited, you can predict which websites I will visit in the future
11. I am often influenced to click on links/websites I didn't initially intend on visiting
12. I don't think it would be difficult to predict my future attitudes, behaviour, and choices

Hours spent online (in hours; open ended question)

Minutes/hours spent online in a single session (open ended question)

Time spent on different social platforms (7-point Likert Scale: 1 = *very little time*, 7 = *a lot of time*)

1. Social media (e.g. Facebook)
2. News websites
3. Blogs
4. Forums
5. Emails
6. Instant messaging
7. Studying (e.g. Google Scholar)
8. Online gaming
9. Online banking
10. Online shopping
11. Other (participants were asked to specify)

Awareness of algorithmic surveillance:

When I'm online I…

1. …notice that pop-ups are related to sites I have previously visited
2. …feel aware that the website I visit have access to my internet history
3. …believe my online data is being shared with other companies and organisations
4. …think that companies profit from selling my online data
5. …notice that even when using the same search term as a friend, we can have completely different search results

6. …notice that the websites I am advertised online are often of a similar theme (e.g. of one type of politics)
7. …notice that website recommendations are related to my gender
8. …feel as though advertisers have made assumptions about who I am
9. …do not feel that I am being tracked
10. …am not aware my private information is being stored
11. …trust organisations to keep my data private from other companies
12. …do not believe organisations share my data
13. …believe I see the same websites advertised online as everyone else
14. …feel my news feed has a wide variety of recommended pages
15. …do not feel that adverts are tailored to certain aspects of myself
16. …do not believe that websites have made judgments on who I am

5. Computer experience (0 = *no experience*, 10 = *a lot of experience*).

a. Coding

b. Hacking

c. Analytics

d. Diagnostics

e. Programming

f. Program installation

Demographics (open ended questions)

a. Age

b. Gender

c. Nationality

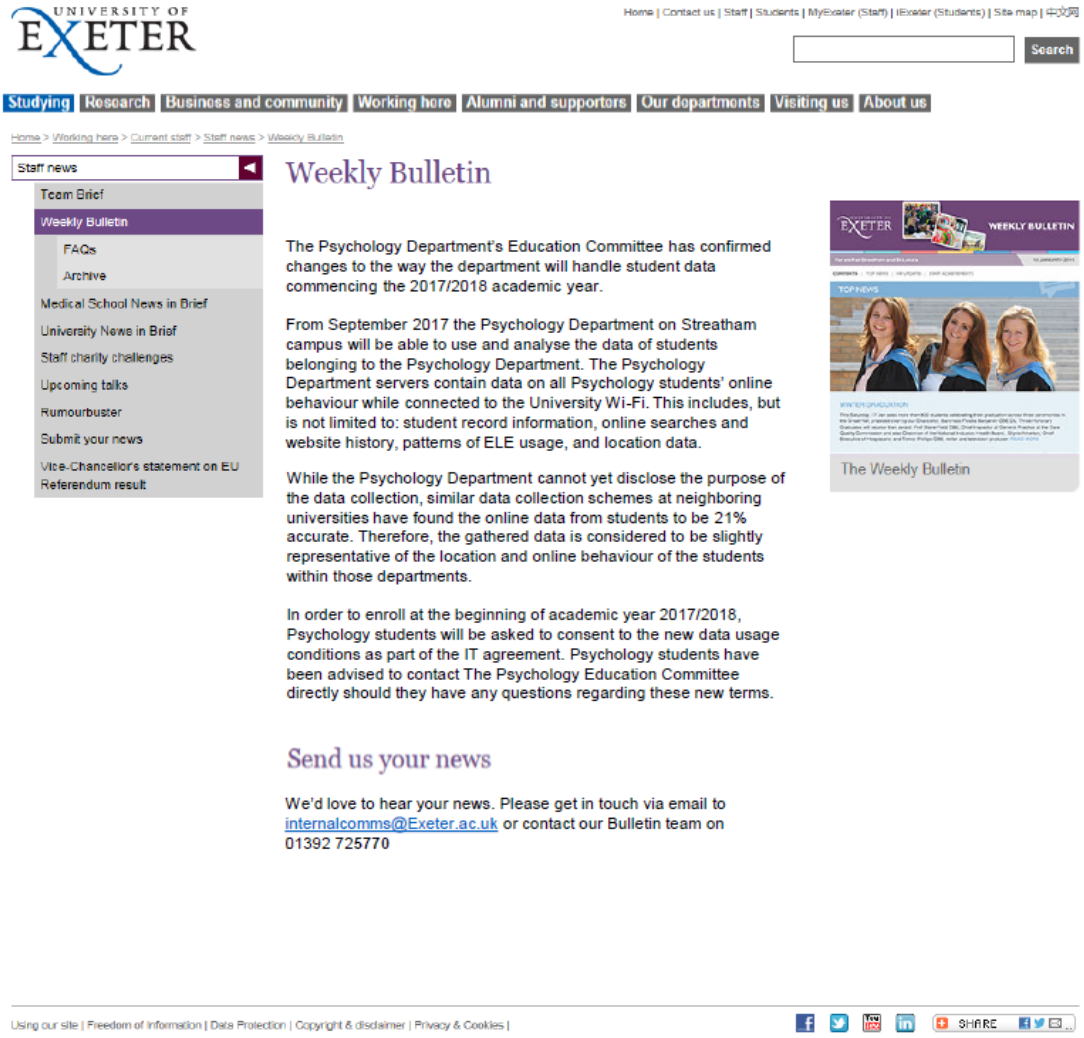
d. Occupation

Article trustworthiness (7-point Likert Scale: 1 = *strongly disagree, 7 = strongly agree)*

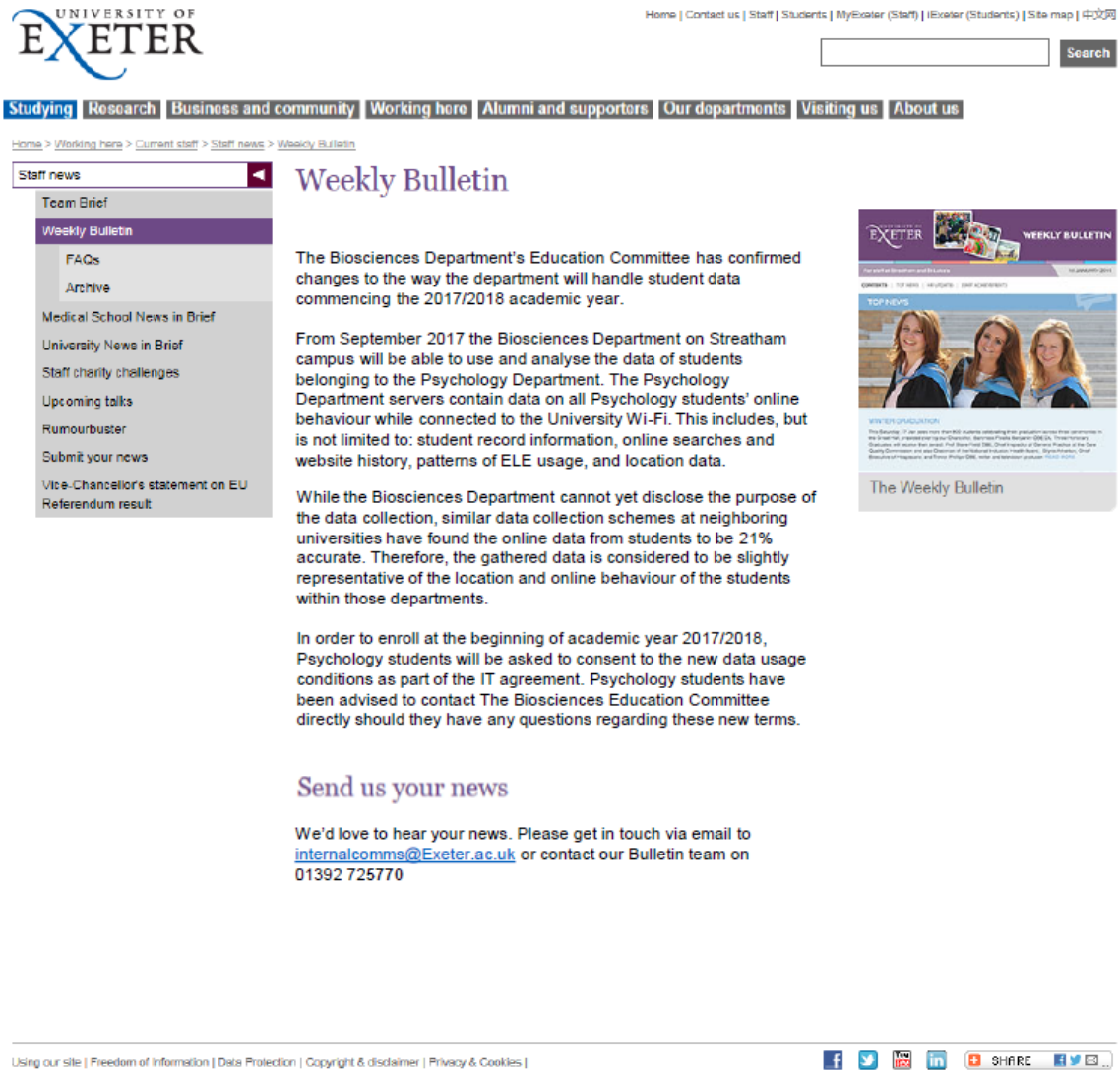
1. The article was trustworthy
2. I believe the article came from a reliable source
3. The information in the article was not believable
4. I would not necessarily believe the news I read from this source

Appendix C: Study 2a manipulation university news bulletin

Condition: Ingroup surveiller, low surveillance accuracy



Condition: Outgroup surveiller, low surveillance accuracy



UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Biosciences Department's Education Committee has confirmed changes to the way the department will handle student data commencing the 2017/2018 academic year.

From September 2017 the Biosciences Department on Streatham campus will be able to use and analyse the data of students belonging to the Psychology Department. The Psychology Department servers contain data on all Psychology students' online behaviour while connected to the University Wi-Fi. This includes, but is not limited to: student record information, online searches and website history, patterns of ELE usage, and location data.

While the Biosciences Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from students to be 21% accurate. Therefore, the gathered data is considered to be slightly representative of the location and online behaviour of the students within those departments.

In order to enroll at the beginning of academic year 2017/2018, Psychology students will be asked to consent to the new data usage conditions as part of the IT agreement. Psychology students have been advised to contact The Biosciences Education Committee directly should they have any questions regarding these new terms.

The Weekly Bulletin

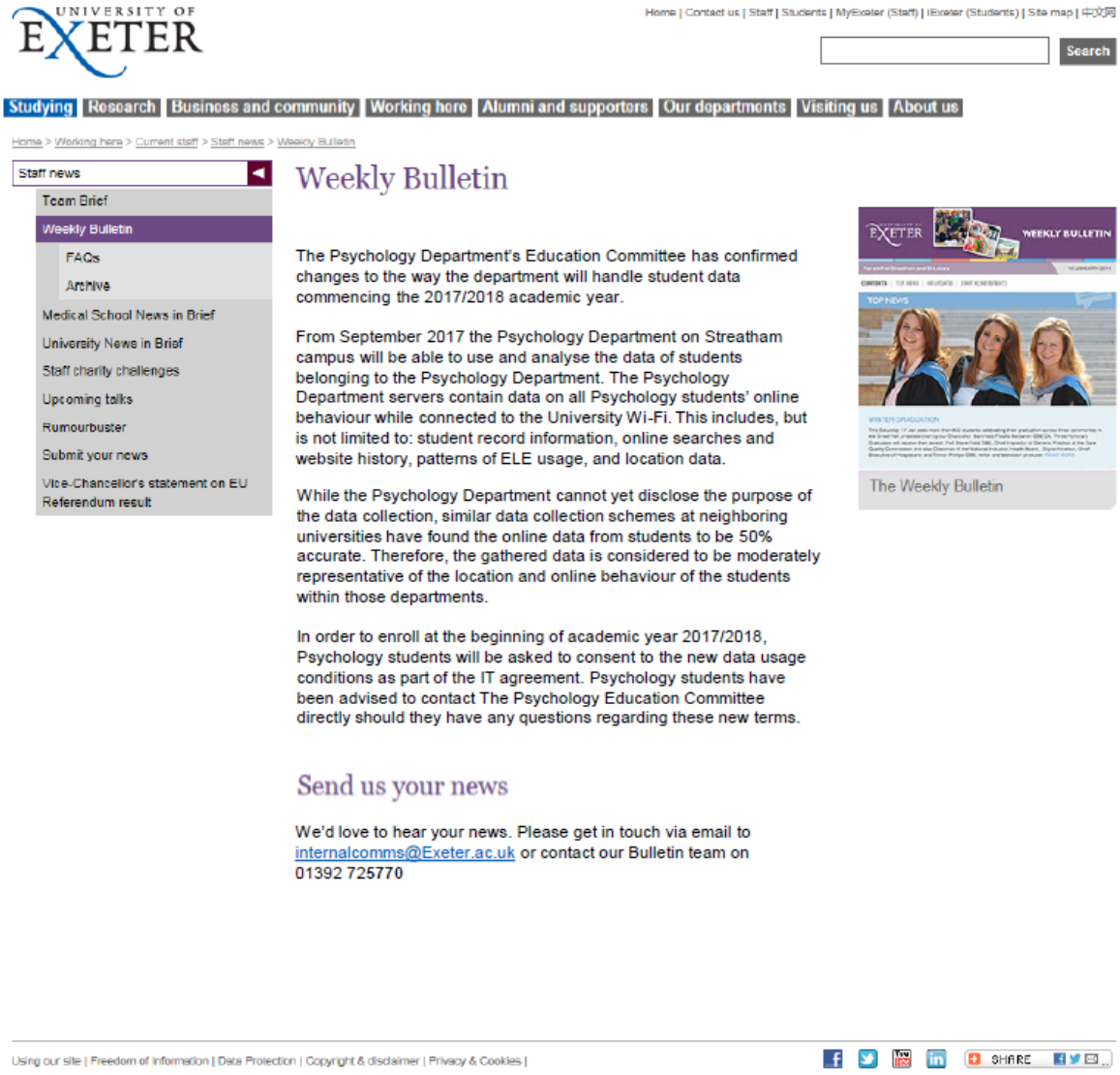
Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

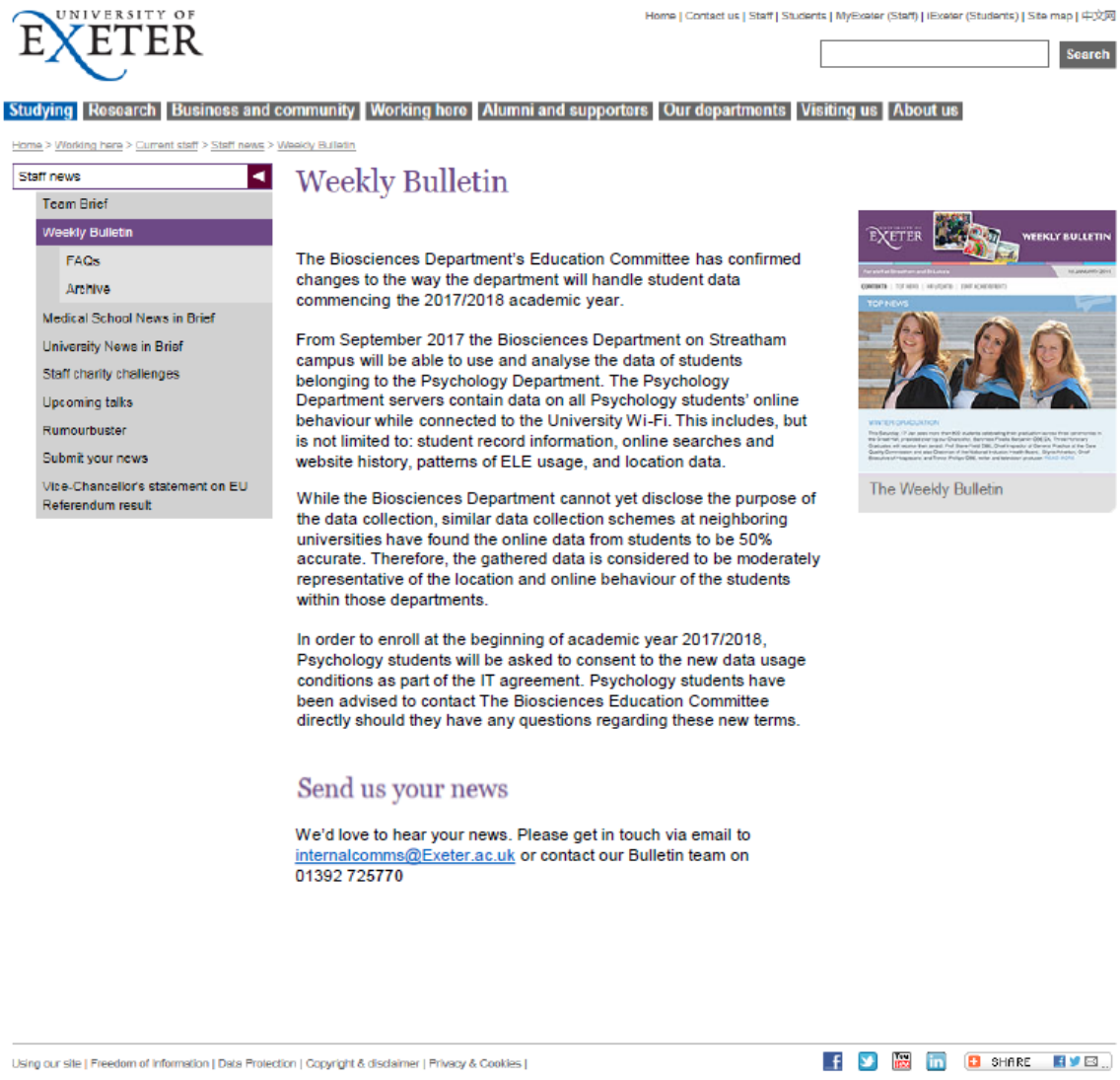
Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

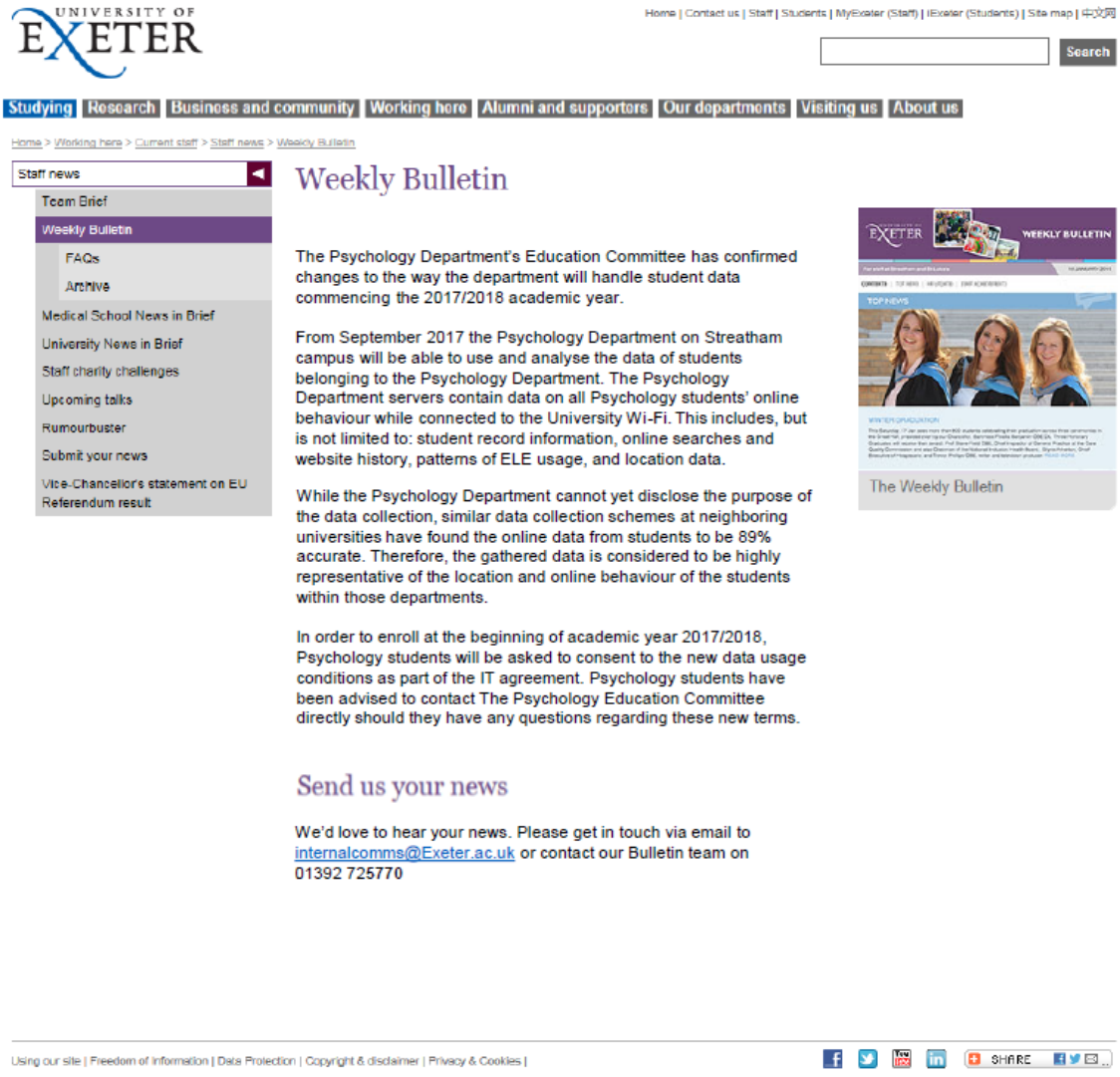
Condition: Ingroup surveiller, medium surveillance accuracy



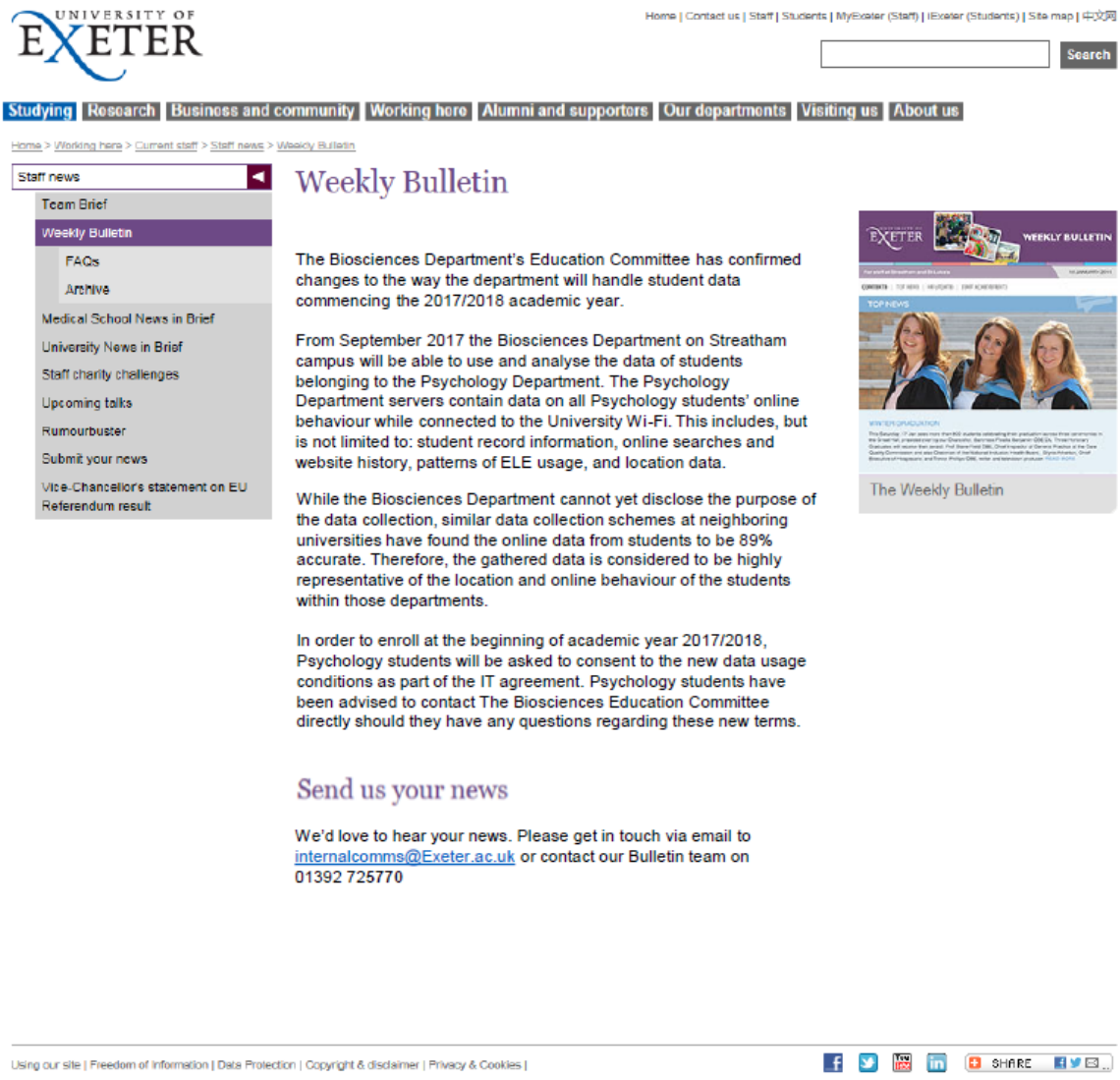
Condition: Outgroup surveiller, medium surveillance accuracy



Condition: Ingroup surveiller, high surveillance accuracy



Condition: Outgroup surveiller, high surveillance accuracy



UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Biosciences Department's Education Committee has confirmed changes to the way the department will handle student data commencing the 2017/2018 academic year.

From September 2017 the Biosciences Department on Streatham campus will be able to use and analyse the data of students belonging to the Psychology Department. The Psychology Department servers contain data on all Psychology students' online behaviour while connected to the University Wi-Fi. This includes, but is not limited to: student record information, online searches and website history, patterns of ELE usage, and location data.

While the Biosciences Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from students to be 89% accurate. Therefore, the gathered data is considered to be highly representative of the location and online behaviour of the students within those departments.

In order to enroll at the beginning of academic year 2017/2018, Psychology students will be asked to consent to the new data usage conditions as part of the IT agreement. Psychology students have been advised to contact The Biosciences Education Committee directly should they have any questions regarding these new terms.

The Weekly Bulletin

Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

Appendix D: Study 2a full list of measures

Accuracy manipulation check:

In my view, the surveillance conducted by the (x) department is…

1. …accurate in identifying students
2. …accurate at determining which sites a student visits online
3. …usually unable to identify students' characteristics
4. …usually unable to know which sites a student visits online

Identification as a psychology student:

1. Overall, being a psychology student has very little to do with how I feel about myself
2. Being a psychology student is an important reflection of who I am
3. In general, being a psychology student is an important part of my self-image
4. Being a psychology student is unimportant to my sense of what kind of person I am

Privacy concern:

1. Surveillance from the (x) department is an invasion of student privacy
2. Psychology students have a right to use the University Wi-Fi without being surveilled

3. It is fair for Psychology students to exchange their online data for the use of University Wi-Fi.
4. Psychology students shouldn't expect privacy when using the University Wi-Fi

Behaviour change intentions online:

Data surveillance from the (x) department would…

1. …make me concerned about what I did while using the University Wi-Fi
2. ...make me censor what I do online while using the University Wi-Fi
3. …not change how I felt about using the University Wi-Fi
4. …not affect what I did online while using the University Wi-Fi

Group-based recognition:

Accuracy:

1. By using psychology student data, the (x) department will accurately understand what a prototypical psychology student is like
2. From analysing psychology student data, it is unlikely that the (x) department would get an accurate picture of what a typical psychology student is like

Distinctiveness:

3. The surveillance program could distinguish how psychology students are unique from students in other departments
4. I do not think psychology student online data could recognise how we are unique from other students

Depth:

5. No matter how much data the (x) department collects, only psychology students understand what it truly means to be a psychology student
6. By using psychology student data, the (x) department could understand psychology students better than I could

Surveiller trust:

1. I trust the intentions of the (x) department
2. Surveillance conducted by the (x) department will be for psychology students' benefit
3. I do not believe the (x) department have good intentions with my data
4. The (x) surveillance programme will not help psychology students

Demographics:

Age (open ended)

Gender:

1. Male
2. Female
3. Other

Nationality:

1. British
2. Other
3. European

Days per week logged on to University Wi-Fi (open ended)

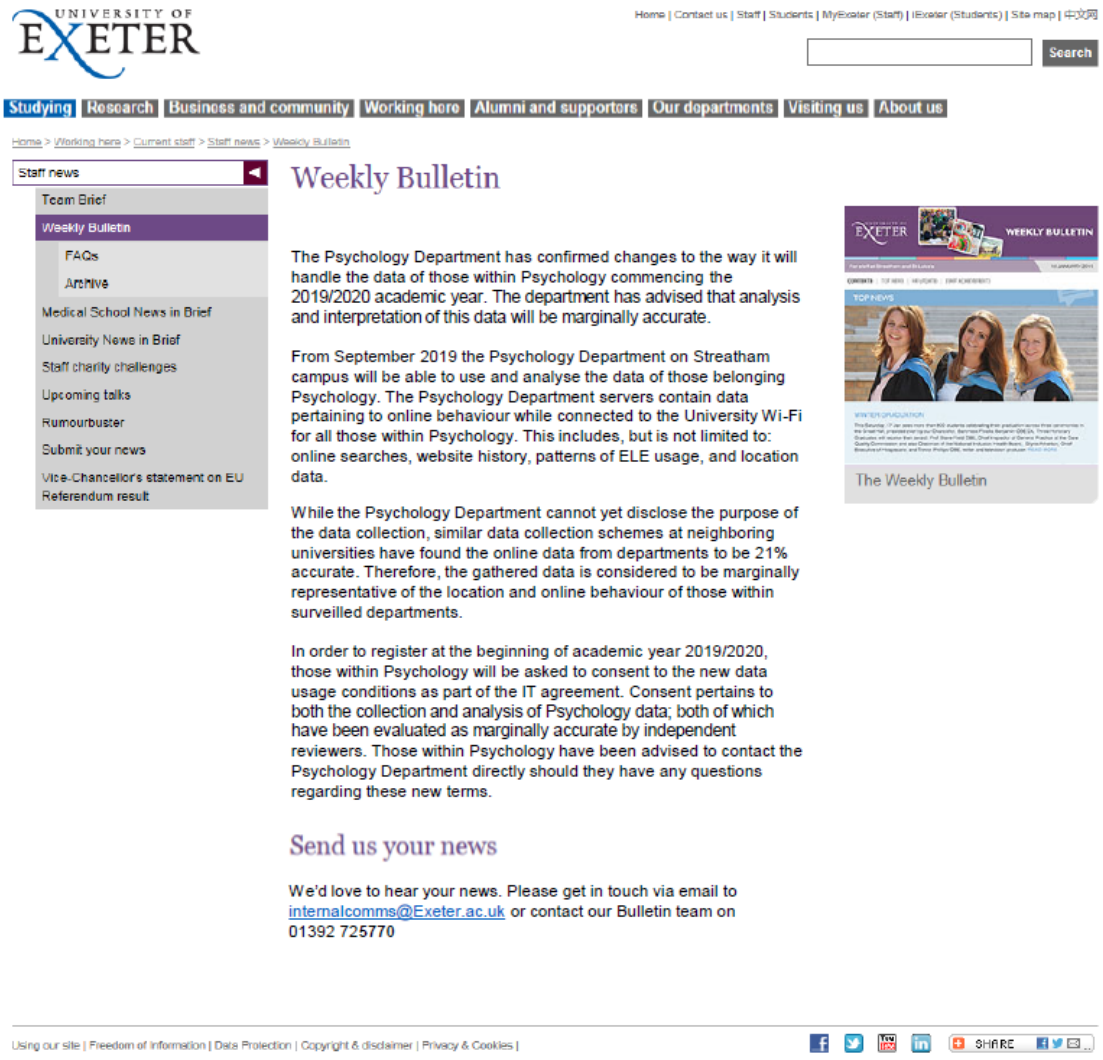
Time in hours logged on to University Wi-Fi per session (open ended)

Trustworthiness of University Bulletin (7-point Likert Scale: 1 = *strongly disagree,* 7 = *strongly agree*):

1. The university news bulletin was trustworthy
2. The information in the news bulletin was not believable

Appendix E: Study 2b manipulation university news bulletin

Condition: Ingroup surveiller, low surveillance accuracy



UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Psychology Department has confirmed changes to the way it will handle the data of those within Psychology commencing the 2019/2020 academic year. The department has advised that analysis and interpretation of this data will be marginally accurate.

From September 2019 the Psychology Department on Streatham campus will be able to use and analyse the data of those belonging Psychology. The Psychology Department servers contain data pertaining to online behaviour while connected to the University Wi-Fi for all those within Psychology. This includes, but is not limited to: online searches, website history, patterns of ELE usage, and location data.

While the Psychology Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from departments to be 21% accurate. Therefore, the gathered data is considered to be marginally representative of the location and online behaviour of those within surveilled departments.

In order to register at the beginning of academic year 2019/2020, those within Psychology will be asked to consent to the new data usage conditions as part of the IT agreement. Consent pertains to both the collection and analysis of Psychology data; both of which have been evaluated as marginally accurate by independent reviewers. Those within Psychology have been advised to contact the Psychology Department directly should they have any questions regarding these new terms.

The Weekly Bulletin

Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

Condition: Outgroup surveiller, low surveillance accuracy

UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Biosciences Department has confirmed changes to the way it will handle the data of those belonging to Psychology commencing the 2019/2020 academic year. The department has advised that analysis and interpretation of this data will be marginally accurate.

From September 2019 the Biosciences Department on Streatham campus will be able to use and analyse the data of those belonging to Psychology. The Biosciences Department servers contain data pertaining to online behaviour while connected to the University Wi-Fi for all those within Psychology. This includes, but is not limited to: online searches, website history, patterns of ELE usage, and location data.

While the Biosciences Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from departments to be 21% accurate. Therefore, the gathered data is considered to be marginally representative of the location and online behaviour of the surveilled departments.

In order to register at the beginning of academic year 2019/2020, all those within Psychology will be asked to consent to the new data usage conditions as part of the IT agreement. Consent pertains to both the collection and analysis of Psychology data; both of which have been evaluated as marginally accurate by independent reviewers. Those within Psychology have been advised to contact The Biosciences Department directly should they have any questions regarding these new terms.

The Weekly Bulletin

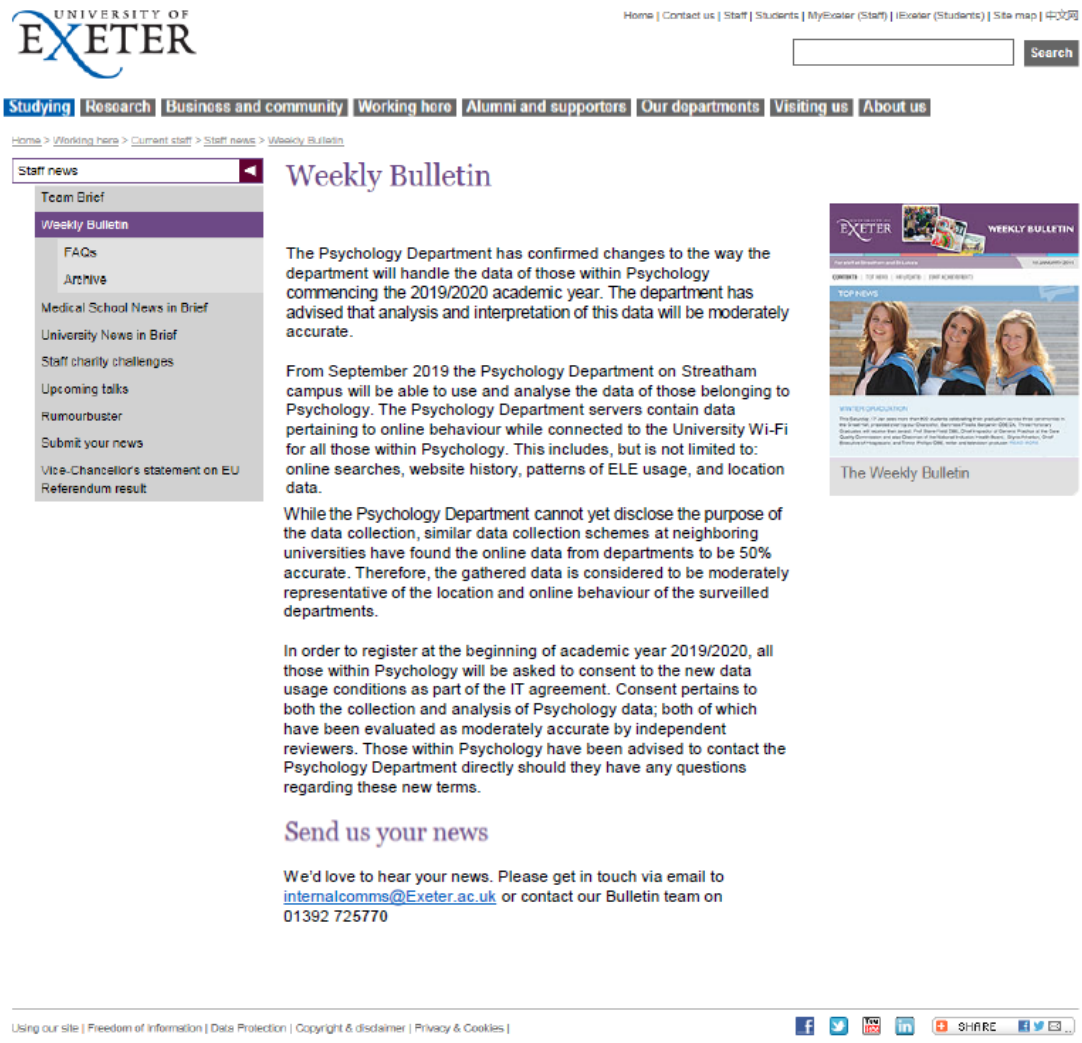
Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

Condition: Ingroup surveiller, medium surveillance accuracy



UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Weekly Bulletin

The Psychology Department has confirmed changes to the way the department will handle the data of those within Psychology commencing the 2019/2020 academic year. The department has advised that analysis and interpretation of this data will be moderately accurate.

From September 2019 the Psychology Department on Streatham campus will be able to use and analyse the data of those belonging to Psychology. The Psychology Department servers contain data pertaining to online behaviour while connected to the University Wi-Fi for all those within Psychology. This includes, but is not limited to: online searches, website history, patterns of ELE usage, and location data.

While the Psychology Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from departments to be 50% accurate. Therefore, the gathered data is considered to be moderately representative of the location and online behaviour of the surveilled departments.

In order to register at the beginning of academic year 2019/2020, all those within Psychology will be asked to consent to the new data usage conditions as part of the IT agreement. Consent pertains to both the collection and analysis of Psychology data; both of which have been evaluated as moderately accurate by independent reviewers. Those within Psychology have been advised to contact the Psychology Department directly should they have any questions regarding these new terms.

Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

Condition: Outgroup surveiller, medium surveillance accuracy

UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Weekly Bulletin

The Biosciences Department has confirmed changes to the way it will handle the data of those belonging to Psychology commencing the 2019/2020 academic year. The department has advised that analysis and interpretation of this data will be moderately accurate.

From September 2019 the Biosciences Department on Streatham campus will be able to use and analyse the data of those belonging to Psychology. The Biosciences Department servers contain data pertaining to online behaviour while connected to the University Wi-Fi for all those within Psychology. This includes, but is not limited to: online searches, website history, patterns of ELE usage, and location data.

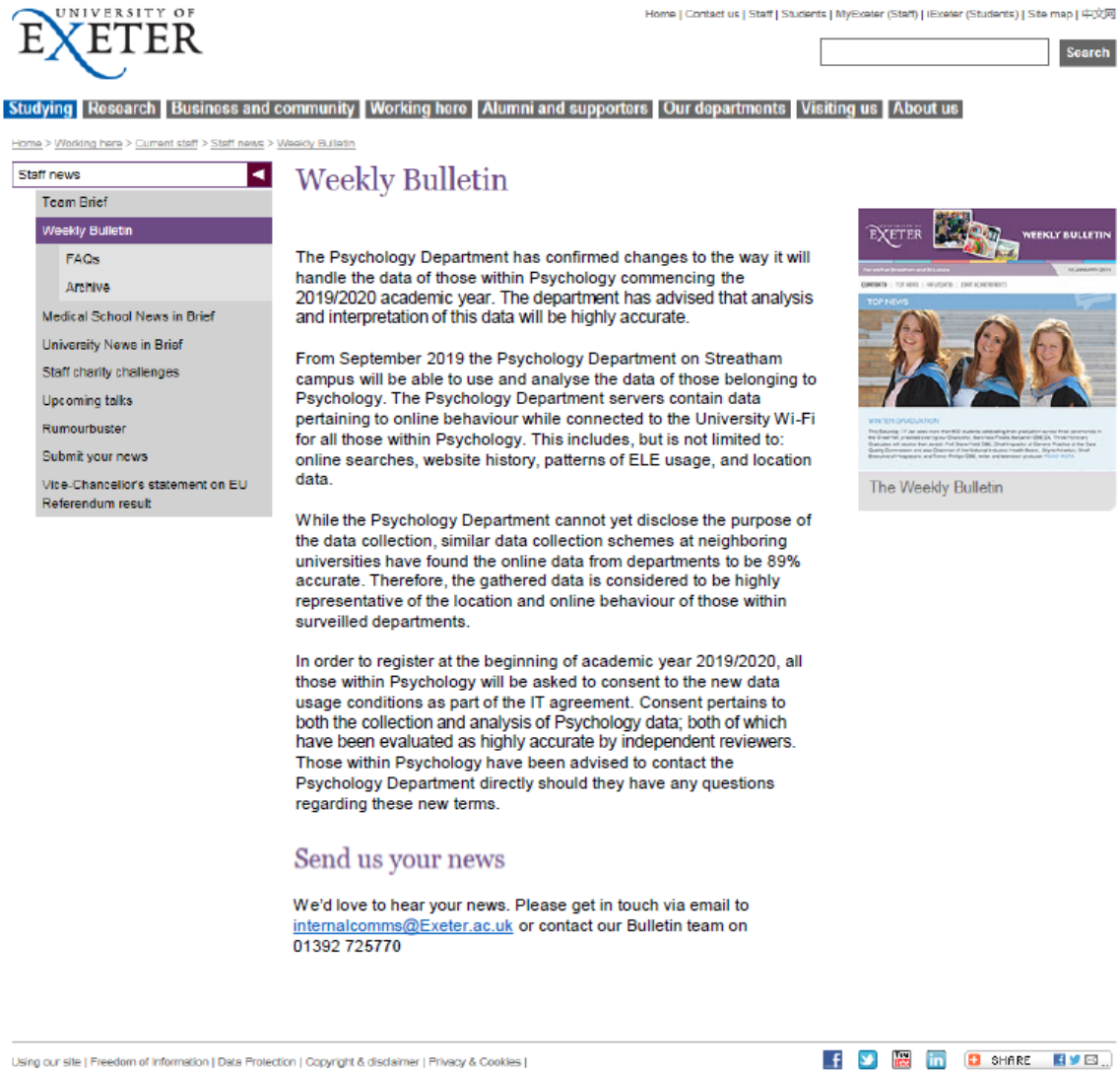
While the Biosciences Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from departments to be 50% accurate. Therefore, the gathered data is considered to be moderately representative of the location and online behaviour of the surveilled departments.

In order to register at the beginning of academic year 2019/2020, all those within Psychology will be asked to consent to the new data usage conditions as part of the IT agreement. Consent pertains to both the collection and analysis of Psychology data; both of which have been evaluated as moderately accurate by independent reviewers. Those within Psychology have been advised to contact The Biosciences Department directly should they have any questions regarding these new terms.

Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Condition: Ingroup surveiller, high surveillance accuracy



UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Psychology Department has confirmed changes to the way it will handle the data of those within Psychology commencing the 2019/2020 academic year. The department has advised that analysis and interpretation of this data will be highly accurate.

From September 2019 the Psychology Department on Streatham campus will be able to use and analyse the data of those belonging to Psychology. The Psychology Department servers contain data pertaining to online behaviour while connected to the University Wi-Fi for all those within Psychology. This includes, but is not limited to: online searches, website history, patterns of ELE usage, and location data.

While the Psychology Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from departments to be 89% accurate. Therefore, the gathered data is considered to be highly representative of the location and online behaviour of those within surveilled departments.

In order to register at the beginning of academic year 2019/2020, all those within Psychology will be asked to consent to the new data usage conditions as part of the IT agreement. Consent pertains to both the collection and analysis of Psychology data; both of which have been evaluated as highly accurate by independent reviewers. Those within Psychology have been advised to contact the Psychology Department directly should they have any questions regarding these new terms.

The Weekly Bulletin

Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

Condition: Outgroup surveiller, high surveillance accuracy

UNIVERSITY OF EXETER

Home | Contact us | Staff | Students | MyExeter (Staff) | iExeter (Students) | Site map | 中文网

Search

Studying | Research | Business and community | Working here | Alumni and supporters | Our departments | Visiting us | About us

Home > Working here > Current staff > Staff news > Weekly Bulletin

Staff news

- Team Brief
- Weekly Bulletin
  - FAQs
  - Archive
- Medical School News in Brief
- University News in Brief
- Staff charity challenges
- Upcoming talks
- Rumourbuster
- Submit your news
- Vice-Chancellor's statement on EU Referendum result

Weekly Bulletin

The Biosciences Department has confirmed changes to the way it will handle the data of those within Psychology commencing the 2019/2020 academic year. The department has advised that analysis and interpretation of this data will be highly accurate.

From September 2019 the Biosciences Department on Streatham campus will be able to use and analyse the data of those belonging to Psychology. The Biosciences Department servers contain data pertaining to online behaviour while connected to the University Wi-Fi for all those within Psychology. This includes, but is not limited to: online searches, website history, patterns of ELE usage, and location data.

While the Biosciences Department cannot yet disclose the purpose of the data collection, similar data collection schemes at neighboring universities have found the online data from departments to be 89% accurate. Therefore, the gathered data is considered to be highly representative of the location and online behaviour of the surveilled departments.

In order to register at the beginning of academic year 2019/2020, all those within Psychology will be asked to consent to the new data usage conditions as part of the IT agreement. Consent pertains to both the collection and analysis of Psychology data; both of which have been evaluated as highly accurate by independent reviewers. Those within Psychology have been advised to contact the Biosciences Department directly should they have any questions regarding these new terms.

The Weekly Bulletin

Send us your news

We'd love to hear your news. Please get in touch via email to internalcomms@Exeter.ac.uk or contact our Bulletin team on 01392 725770

Using our site | Freedom of Information | Data Protection | Copyright & disclaimer | Privacy & Cookies |

SHARE

Appendix F: Study 2b full list of measures

Accuracy manipulation check:

In my view, algorithmic surveillance conducted by the (x) Department...

1. ...is accurate at identifying people
2. ...creates an accurate impression of people
3. ...does not identify people's characteristics accurately
4. ...does not create an accurate impression of people

Group-based recognition

Distinctiveness:

1. Algorithmic surveillance will enable the (x) Department to recognise that we are a unique discipline
2. Algorithmic surveillance will not recognise our unique characteristics
3. From using algorithmic surveillance, the (x) Department will recognise that we are unique from those belonging to other disciplines
4. Algorithmic surveillance conducted by the (x) Department would imply that we are indistinguishable from other academic communities

Perceived stereotyping:

1. From using algorithmic surveillance, the (x) Department would recognise that we are a diverse community
2. The surveillance programme would suggest that we are all the same

Positivity:

1. The results of algorithmic surveillance from the (x) Department would offer a positive image of us
2. Algorithmic surveillance conducted by the (x) Department would not portray us positively
3. The surveillance programme will help promote the positive impact we have within the University
4. We will be valued positively through the surveillance programme

Understanding:

1. Algorithmic surveillance will not provide the (x) Department with an accurate understanding of our culture
2. Algorithmic surveillance will help the (x) Department understand our values
3. Algorithmic surveillance will provide the (x) Department with a good understanding of what we think
4. Algorithmic surveillance will not provide a better understanding of our views

Identification as a group member:

1. Through algorithmic surveillance, I believe I would be identified as belonging to Psychology
2. Algorithmic surveillance would not identify me as part of Psychology

Feelings towards surveillance:

The (x) Department's surveillance programme makes me feel:

1. Worried
2. Calm
3. Anxious
4. Relaxed
5. Angry
6. Happy
7. Annoyed
8. Pleased
9. Uncomfortable
10. Comfortable
11. Hopeful
12. Dejected
13. Optimistic
14. Discouraged

Visibility (participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how the surveillance programme made them feel):

1. Invisible/Visible
2. Anonymous/Identifiable
3. Unobserved/Observed
4. Unknown/Known

Surveiller trust:

1. I trust the (x) Department to gather our online data
2. Surveillance conducted online by the (x) Department is for our benefit
3. I do not believe the (x) Department have good intentions with our data
4. The surveillance programme will not benefit us

Privacy concern:

1. Surveillance online is an invasion of privacy
2. People have a right to use the internet without being surveilled
3. People's online data should not be private information
4. People shouldn't expect privacy when using the internet

Behaviour change intentions:

Algorithmic surveillance would…

1. …make me concerned about what I do online
2. …make me censor what I do online
3. …not change how I use the internet
4. …not affect what I do online

Demographics:

Current course of study

1. Psychology
2. Clinical Psychology

3. Flexible combined honours (with Psychology)
4. Other Psychology course
5. Non-Psychology course

Hours per week spent online (open ended)

Age (open ended)

Gender

1. Man
2. Woman
3. Non-binary
4. Prefer not to say

Ethnicity

1. White
2. Mixed/Multiple ethnic groups
3. Asian/Asian British
4. Black/African/Caribbean/Black British
5. Arab
6. Other (open ended)

Membership to closed or private groups/forums online

1. Yes
2. No

Awareness of algorithmic surveillance (1-10: 1 = not at all aware, 10 = very aware)

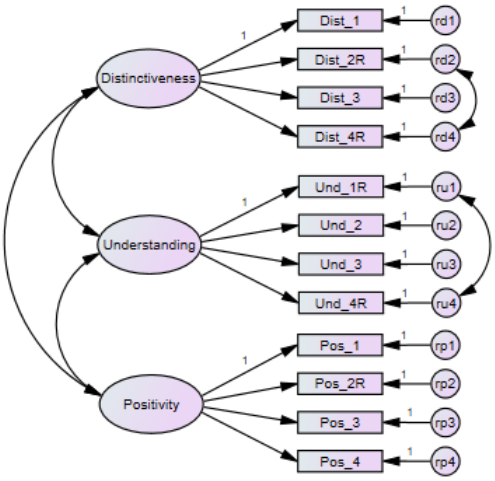
Trustworthiness of news bulletin (7-point Likert scale: 1 = *strongly disagree,* 7 = *strongly agree)*

Appendix G: Confirmatory factor analysis for the group-based recognition scale

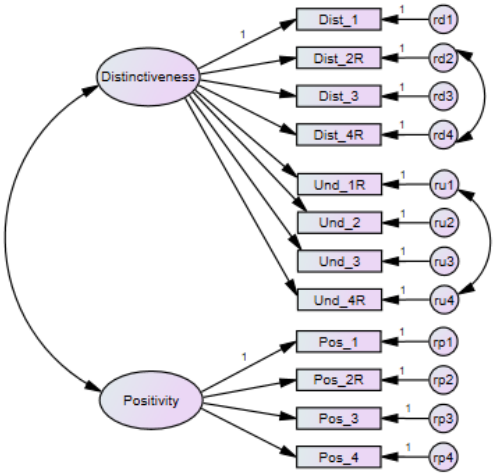
Confirmatory factor analysis was conducted to compare the hypothesised three-dimension structure (Model 1) with two variants of a more parsimonious two-dimension structure (Model 1a and Model 1b). Reverse coded items were covaried within each dimension to account for shared method variance.

Model 1 was tested as a baseline that could be compared with the two-dimension models. Model 1 demonstrated acceptable fit, $\chi^2_{49} = 183.4$, $p < .001$, $\chi^2/df = 3.74$, TLI = .783, CFI = .839, RMSEA = .117, AIC = 241.38. Model 1a was then tested, which demonstrated poor fit, $\chi^2_{51} = 265.22$, $p < .001$, $\chi^2/df = 5.20$, TLI = .668, CFI = .743, RMSEA = .145, AIC = 319.22, and had significantly worse fit when compared with Model 1, $\Delta\chi^2_2 = 81.82$, $p < .001$, ΔAIC = 77.84.

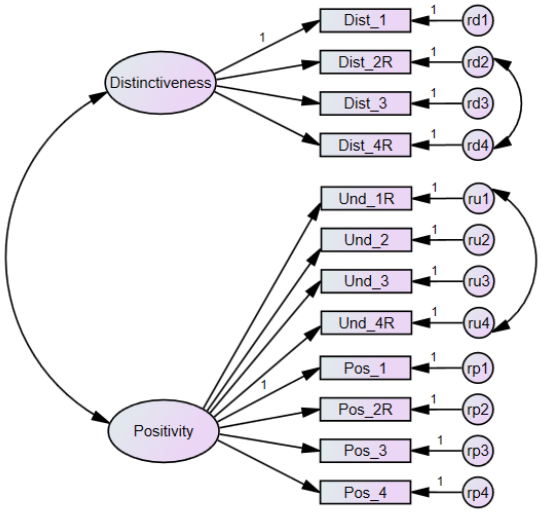
Model 1b was then tested and demonstrated poor fit, $\chi^2_{51} = 232.10$, $p < .001$, $\chi^2/df = 4.55$, TLI = .719, CFI = .783, RMSEA = .134, AIC = 286.10. This was significantly poorer than the three-dimension Model 1, $\Delta\chi^2_2 = 48.70$, $p < .001$, ΔAIC = 44.72. As such, Model 1 was considered the superior model.



Model 1



Model 1a



Model 1b

Appendix H: Study 2c manipulation article

Page 1. Condition: Ingroup surveiller, low surveillance accuracy

Surveillance

British people are under highly inaccurate surveillance from British intelligence

New leaks reveal that our intelligence service, GCHQ, is conducting extensive yet highly inaccurate surveillance on the public. Wired speaks to an industry expert.

By **SAM BURGE**

Wednesday 28 June, 2017

GCHQ in Cheltenham, Gloucestershire

Credit: Ministry of Defence/Wikipedia

Leaked documents have been published that reveal the specific algorithms used by GCHQ to surveil British people online. These documents have now given analysts the opportunity to assess how effective these algorithms actually are. The verdict is in: British intelligence monitors our online behaviour with very little precision.

Whilst GCHQ have refused to comment, an independent industry expert (who wishes to remain anonymous) has stated:

'Our analyses suggest that the data collected by GCHQ is not at all representative of the British population. In other words, if they want to know something about the British people, their surveillance will give them a very poor understanding.'

This misguided knowledge of our online activity results from their algorithms. Put simply, algorithms are chunks of code that can process large amounts of data (or data from a lot of people) very quickly. This means that the gaze of GCHQ isn't focussed on a handful of particular people, but every British citizen with access to the internet.

Page 2. Condition: Ingroup surveiller, low surveillance accuracy

READ NEXT

WIRED's guide to 25 of the best films on Netflix UK

By WIRED

READ NEXT

Modifying human cells to create "anti-leukaemia soldiers"

Their algorithms provide them with an entirely false picture of what an average British person is doing online

Anonymous, from within the intelligence community

'Yet despite GCHQ hoovering up our data, their algorithms provide them with an entirely false picture of what an average British person is doing online. GCHQ's algorithms pour over everyone's data looking for patterns. Specifically, they try and find patterns in our online behaviour; what sites are people typically visiting? What products are people usually buying? What social media posts are people reading? And so on. It turns out GCHQ is remarkable poor at piecing this puzzle together'.

Despite their silence, GCHQ have not challenged the authenticity of the leaked document. However, what we can be sure of is that whatever GCHQ have on us, it can give a highly inaccurate insight into British online behaviour.

This article was first published in the July 2017 issue of WIRED magazine

VIEW ISSUE

SURVEILLANCE PRIVACY MASS SURVEILLANCE

SHARE THIS ARTICLE

RECOMMENDED

Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem

By MATT BURGESS

Earth Day 2017: what is it and why is it important?

By ALEXANDRA SIMON-LEWIS

What is the EmDrive and why is it so controversial?

By ERIC HUTSON

Trick of the light: Nanjing's trippy cultural centre is a mass of optical illusions

By PAULINE BOCK

Page 1. Condition: Outgroup surveiller, low surveillance accuracy

Surveillance

British people are under highly inaccurate surveillance from American intelligence

New leaks reveal that the American intelligence service, the NSA, is conducting extensive yet highly inaccurate surveillance on the public. Wired speaks to an industry expert.

By **SAM BURGE**

Wednesday 28 June, 2017

The headquarters of the National Security Agency (NSA) in Fort Meade, Maryland.
JIM LO SCALZO/EPA/REDUX

Leaked documents have been published that reveal the specific algorithms used by the NSA to surveil British people online. These documents have now given analysts the opportunity to assess how effective these algorithms actually are. The verdict is in: American intelligence monitors our online behaviour with very little precision.

Whilst the NSA have refused to comment, an independent industry expert (who wishes to remain anonymous) has stated:

'Our analyses suggest that the data collected by the NSA is not at all representative of the British population. In other words, if they want to know something about the British people, their surveillance will give them a very poor understanding.'

This misguided knowledge of our online activity results from their algorithms. Put simply, algorithms are chunks of code that can process large amounts of data (or data from a lot of people) very quickly. This means that the gaze of the NSA isn't focussed on a handful of particular people, but every British citizen with access to the internet.

Page 2. Condition: Outgroup surveiller, low surveillance accuracy

READ NEXT

WIRED's guide to 25 of the best films on Netflix UK

By WIRED

READ NEXT

Modifying human cells to create "anti-leukaemia soldiers"

Their algorithms provide them with an entirely false picture of what an average British person is doing online

Anonymous, from within the intelligence community

'Yet despite the NSA hoovering up our data, their algorithms provide them with an entirely false picture of what an average British person is doing online. The NSA's algorithms pour over everyone's data looking for patterns. Specifically, they try and find patterns in our online behaviour; what sites are people typically visiting? What products are people usually buying? What social media posts are people reading? And so on. It turns out the NSA is remarkable poor at piecing this puzzle together'.

Despite their silence, the NSA have not challenged the authenticity of the leaked document. However, what we can be sure of is that whatever the NSA have on us, it can give a highly inaccurate insight into British online behaviour.

This article was first published in the July 2017 issue of WIRED magazine

VIEW ISSUE

SURVEILLANCE PRIVACY MASS SURVEILLANCE

SHARE THIS ARTICLE

RECOMMENDED

Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem

By MATT BURGESS

Earth Day 2017: what is it and why is it important?

By ALEXANDRA SIMON-LEWIS

What is the EmDrive and why is it so controversial?

By ERIC HUTSON

Trick of the light: Nanjing's trippy cultural centre is a mass of optical illusions

By PAULINE BOCK

Page 1. Condition: Ingroup surveiller, medium surveillance accuracy

WIRED Technology | Science | Culture | Video | Reviews | Magazine | More | Follow

The best designer watches
2 days ago | 6 items

Data doesn't lie: tech firms need to hire more women to succeed
2 days ago

The next Daesh is coming to a news feed near you in 2018
2 days ago

Travel in style on land, sea and in the skies with the best luxury rides
5 days ago | 6 items

Surveillance

British people are under surveillance from British intelligence, yet its accuracy is questionable

New leaks reveal that our intelligence service, GCHQ, is conducting extensive, yet inconsistent surveillance on the public. Wired speaks to an industry expert.

By **SAM BURGE**

Wednesday 28 June, 2017

GCHQ in Cheltenham, Gloucestershire

Credit: Ministry of Defence/Wikipedia

Leaked documents have been published that reveal the specific algorithms used by GCHQ to surveil British people online. These documents have now given analysts the opportunity to assess how effective these algorithms actually are. The verdict is mixed: British intelligence monitors our online behaviour with variable accuracy.

Whilst GCHQ have refused to comment, an independent industry expert (who wishes to remain anonymous) has stated:
'Our analyses suggest that the data collected by GCHQ provides a slightly blurred impression of the British population. In other words, if they want to know something about the British people, their surveillance will only sometimes give them a reliable answer.'

This vague knowledge of our online activity is provided by their algorithms. Put simply, algorithms are chunks of code that can process large amounts of data (or data from a lot of people) very quickly. This means that the gaze of GCHQ isn't focussed on a handful of particular people, but every British citizen with access to the internet.

Page 2. Condition: Ingroup surveiller, medium surveillance accuracy

READ NEXT

WIRED's guide to 25 of the best films on Netflix UK

By WIRED

READ NEXT

Modifying human cells to create "anti-leukaemia soldiers"

Their algorithms only enable them to build a somewhat murky picture of what an average British person is doing online

Anonymous, from within the intelligence community

'Yet despite GCHQ hoovering up our data, their algorithms only enable them to build a somewhat murky picture of what an average British person is doing online. GCHQ's algorithms pour over everyone's data looking for patterns. Specifically, they try and find patterns in our online behaviour; what sites are people typically visiting? What products are people usually buying? What social media posts are people reading? And so on. It turns out GCHQ can sometimes piece this puzzle together'.

Despite their silence, GCHQ have not challenged the authenticity of the leaked document. However, what we can be sure of is that whatever GCHQ have on us, it only occasionally gives an accurate insight into British online behaviour.

This article was first published in the July 2017 issue of WIRED magazine

VIEW ISSUE

SURVEILLANCE PRIVACY MASS SURVEILLANCE

SHARE THIS ARTICLE

RECOMMENDED

Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem

By MATT BURGESS

Earth Day 2017: what is it and why is it important?

By ALEXANDRA SIMON-LEWIS

What is the EmDrive and why is it so controversial?

By ERIC HUTSON

Trick of the light: Nanjing's trippy cultural centre is a mass of optical illusions

By PAULINE BOCK

Page 1. Condition: Outgroup surveiller, medium surveillance accuracy

Surveillance

British people are under surveillance from American intelligence, yet its accuracy is questionable

New leaks reveal that the intelligence service, the NSA, is conducting extensive, yet inconsistent surveillance on the public. Wired speaks to an industry expert.

By **SAM BURGE**

Wednesday 28 June, 2017

The headquarters of the National Security Agency (NSA) in Fort Meade, Maryland.
JIM LO SCALZO/EPA/REDUX

Leaked documents have been published that reveal the specific algorithms used by the NSA to surveil British people online. These documents have now given analysts the opportunity to assess how effective these algorithms actually are. The verdict is mixed: American intelligence monitors our online behaviour with variable accuracy.

Whilst the NSA have refused to comment, an independent industry expert (who wishes to remain anonymous) has stated:
'Our analyses suggest that the data collected by the NSA provides a slightly blurred impression of the British population. In other words, if they want to know something about the British people, their surveillance will only sometimes give them a reliable answer.'

This vague knowledge of our online activity is provided by their algorithms. Put simply, algorithms are chunks of code that can process large amounts of data (or data from a lot of people) very quickly. This means that the gaze of the NSA isn't focussed on a handful of particular people, but every British citizen with access to the internet.

Page 2. Condition: Outgroup surveiller, medium surveillance accuracy

READ NEXT

WIRED's guide to 25 of the best films on Netflix UK

By WIRED

READ NEXT

Modifying human cells to create "anti-leukaemia soldiers"

Their algorithms only enable them to build a somewhat murky picture of what an average British person is doing online

Anonymous, from within the intelligence community

'Yet despite the NSA hoovering up our data, their algorithms only enable them to build a somewhat murky picture of what an average British person is doing online. The NSA's algorithms pour over everyone's data looking for patterns. Specifically, they try and find patterns in our online behaviour; what sites are people typically visiting? What products are people usually buying? What social media posts are people reading? And so on. It turns out the NSA can sometimes piece this puzzle together'.

Despite their silence, the NSA have not challenged the authenticity of the leaked document. However, what we can be sure of is that whatever the NSA have on us, it only occasionally gives an accurate insight into British online behaviour.

This article was first published in the July 2017 issue of WIRED magazine

VIEW ISSUE

SURVEILLANCE PRIVACY MASS SURVEILLANCE

SHARE THIS ARTICLE

RECOMMENDED

Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem

By MATT BURGESS

Earth Day 2017: what is it and why is it important?

By ALEXANDRA SIMON-LEWIS

What is the EmDrive and why is it so controversial?

By ERIC HUTSON

Trick of the light: Nanjing's trippy cultural centre is a mass of optical illusions

By PAULINE BOCK

Page 1. Condition: Ingroup surveiller, high surveillance accuracy

Surveillance

British people are under highly accurate surveillance from British intelligence

New leaks reveal that our intelligence service, GCHQ, is conducting extensive and highly accurate surveillance on the public. Wired speaks to an industry expert.

By **SAM BURGE**

Wednesday 28 June, 2017

GCHQ in Cheltenham, Gloucestershire

Credit: Ministry of Defence/Wikipedia

Leaked documents have been published that reveal the specific algorithms used by GCHQ to surveil British people online. These documents have now given analysts the opportunity to assess how effective these algorithms actually are. The verdict is in: British intelligence can monitor our online behaviour with very high precision.

Whilst GCHQ have refused to comment, an independent industry expert (who wishes to remain anonymous) has stated:

'Our analyses suggest that the data collected by GCHQ is highly representative of the British population. In other words, if they want to know something about the British people, their surveillance allows them to get a very reliable answer.'

This exact knowledge of our online activity is only possible through their algorithms. Put simply, algorithms are chunks of code that can process large amounts of data (or data from a lot of people) very quickly. This means that the gaze of GCHQ isn't focussed on a handful of particular people, but every British citizen with access to the internet.

Page 2. Condition: Ingroup surveiller, high surveillance accuracy

READ NEXT

WIRED's guide to 25 of the best films on Netflix UK

By WIRED

READ NEXT

Modifying human cells to create "anti-leukaemia soldiers"

Their algorithms also enable them to build a perfectly clear picture of what an average British person is doing online

Anonymous, from within the intelligence community

'So GCHQ are not only hoovering up our data, their algorithms also enable them to build a perfectly clear picture of what an average British person is doing online. GCHQ's algorithms pour over everyone's data looking for patterns. Specifically, they try and find patterns in our online behaviour; what sites are people typically visiting? What products are people usually buying? What social media posts are people reading? And so on. It turns out GCHQ is remarkable good at piecing this puzzle together'.

Despite their silence, GCHQ have not challenged the authenticity of the leaked document. However, what we can be sure of is that whatever GCHQ have on us, it can give a highly accurate insight into British online behaviour.

This article was first published in the July 2017 issue of WIRED magazine

VIEW ISSUE

SURVEILLANCE PRIVACY MASS SURVEILLANCE

SHARE THIS ARTICLE

RECOMMENDED

Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem

By MATT BURGESS

Earth Day 2017: what is it and why is it important?

By ALEXANDRA SIMON-LEWIS

What is the EmDrive and why is it so controversial?

By ERIC HUTSON

Trick of the light: Nanjing's trippy cultural centre is a mass of optical illusions

By PAULINE DOCK

Page 1. Condition: Outgroup surveiller, high surveillance accuracy

Surveillance

British people are under highly accurate surveillance from American intelligence

New leaks reveal that the American intelligence service, the NSA, is conducting extensive and highly accurate surveillance on the public. Wired speaks to an industry expert.

By **SAM BURGE**

Wednesday 28 June, 2017

The headquarters of the National Security Agency (NSA) in Fort Meade, Maryland.
JIM LO SCALZO/EPA/REDUX

Leaked documents have been published that reveal the specific algorithms used by the NSA to surveil British people online. These documents have now given analysts the opportunity to assess how effective these algorithms actually are. The verdict is in: American intelligence can monitor our online behaviour with very high precision.

Whilst the NSA have refused to comment, an independent industry expert (who wishes to remain anonymous) has stated:

'Our analyses suggest that the data collected by the NSA is highly representative of the British population. In other words, if they want to know something about the British people, their surveillance allows them to get a very reliable answer.'

This exact knowledge of our online activity is only possible through their algorithms. Put simply, algorithms are chunks of code that can process large amounts of data (or data from a lot of people) very quickly. This means that the gaze of the NSA isn't focussed on a handful of particular people, but every British citizen with access to the internet.

Page 2. Condition: Outgroup surveiller, high surveillance accuracy

READ NEXT

WIRED's guide to 25 of the best films on Netflix UK

By WIRED

READ NEXT

Modifying human cells to create "anti-leukaemia soldiers"

Their algorithms also enable them to build a perfectly clear picture of what an average British person is doing online

Anonymous, from within the intelligence community

'So the NSA are not only hoovering up our data, their algorithms also enable them to build a perfectly clear picture of what an average British person is doing online. The NSA's algorithms pour over everyone's data looking for patterns. Specifically, they try and find patterns in our online behaviour; what sites are people typically visiting? What products are people usually buying? What social media posts are people reading? And so on. It turns out the NSA are remarkable good at piecing this puzzle together'.

Despite their silence, the NSA have not challenged the authenticity of the leaked document. However, what we can be sure of is that whatever the NSA have on us, it can give a highly accurate insight into British online behaviour.

This article was first published in the July 2017 issue of WIRED magazine

VIEW ISSUE

SURVEILLANCE PRIVACY MASS SURVEILLANCE

SHARE THIS ARTICLE

RECOMMENDED

Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem

By MATT BURGESS

Earth Day 2017: what is it and why is it important?

By ALEXANDRA SIMON-LEWIS

What is the EmDrive and why is it so controversial?

By ERIC HUTSON

Trick of the light: Nanjing's trippy cultural centre is a mass of optical illusions

By PAULINE BOCK

Appendix I: Study 2c full list of measures

Accuracy manipulation:

1. The *Wired* article suggests that algorithmic surveillance is…
2. After reading the article, in my opinion algorithmic surveillance is…

Group-based recognition:

Distinctiveness:

1. Algorithmic surveillance enables (x) to recognise that British people's beliefs are distinct from those of other nationalities
2. Algorithmic surveillance from (x) suggests that the characteristics of British people are the same as those from other nationalities
3. From using algorithmic surveillance, (x) recognises that British people have distinct characteristics
4. Algorithmic surveillance conducted by (x) does not suggest that the British are unique

Positivity:

1. The results of algorithmic surveillance by (x) offers a positive image of British people
2. Algorithmic surveillance conducted by (x) is very unlikely to portray British people positively

Understanding

1. Algorithmic surveillance does not provide (x) with an accurate understanding of British culture
2. Algorithmic surveillance helps (x) to understand British cultural values
3. Algorithmic surveillance provides (x) with a good understanding of what British people think
4. Algorithmic surveillance does not provide (x) with a better understanding of British people's views

Feelings towards surveillance:

Algorithmic surveillance makes me feel:

1. Worried
2. Calm
3. Anxious
4. Relaxed
5. Angry
6. Happy
7. Annoyed
8. Pleased
9. Uncomfortable
10. Comfortable
11. Hopeful
12. Dejected
13. Optimistic
14. Discouraged

Visibility (participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how algorithmic surveillance made them feel):

1. Invisible/Visible
2. Anonymous/Identifiable
3. Unobserved/Observed
4. Unknown/Known

Surveiller trust:

1. I trust (x) to gather British people's online data
2. Surveillance conducted online by (x) is for the benefit of British people
3. I do not believe (x) have good intentions with British people's data
4. Surveillance online from (x) will not benefit British people

Privacy concern:

1. Surveillance online is an invasion of privacy
2. People have a right to use the internet without being surveilled
3. People's online data should not be private information
4. People shouldn't expect privacy when using the internet

Behaviour change intentions:

Algorithmic surveillance would…

1. …make me concerned about what I do online
2. …make me censor what I do online
3. …not change how I use the internet
4. …not affect what I do online

Demographics:

Hours per week spent online (open ended)

Age (open ended)

Gender

1. Man
2. Woman
3. Non-binary
4. Prefer not to say

Ethnicity

1. White
2. Mixed/Multiple ethnic groups
3. Asian/Asian British
4. Black/African/Caribbean/Black British
5. Arab
6. Other (open ended)

Membership to closed or private groups/forums online

1. Yes
2. No

Awareness of algorithmic surveillance (1-10: 1 = *not at all aware,* 10 = *very aware*).

Trustworthiness of article (7-point Likert scale: 1 = *strongly disagree,* 7 = *strongly agree*):

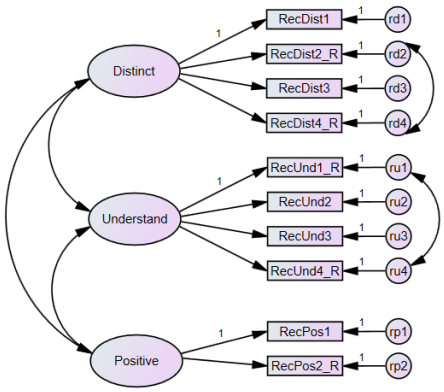
1. The article was trustworthy
2. The information in the article was not believable

Appendix J: Confirmatory factor analysis for the group-based recognition measure

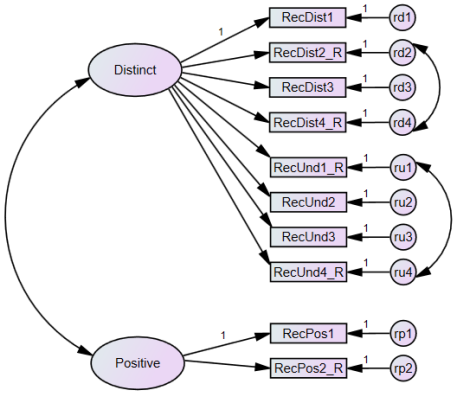
Confirmatory factor analysis was conducted to compare the hypothesised three-dimension structure (Model 1) with two variants of a more parsimonious two-dimension structure (Model 1a and Model 1b). Reverse coded items were covaried within each dimension to account for shared method variance.

Model 1 was tested as a baseline that could be compared with the two-dimension models. Model 1 demonstrated acceptable fit, $\chi^2_{30} = 99.31$, $p < .001$, $\chi^2/df = 3.31$, TLI = .828, CFI = .885, RMSEA = .098, AIC = 149.31. Model 1a was then tested, which demonstrated poor fit, $\chi^2_{32} = 180.38$, $p < .001$, $\chi^2/df = 5.64$, TLI = .655, CFI = .754, RMSEA = .138, AIC = 226.38, and had significantly worse fit when compared with Model 1, $\Delta\chi^2_2 = 81.08$, $p < .001$, ΔAIC = 77.07.

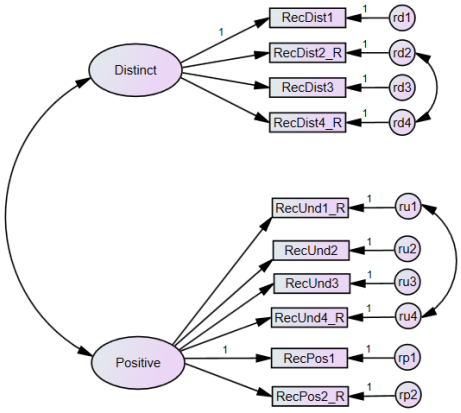
Model 1b was then tested and demonstrated adequate fit, $\chi^2_{32} = 114.14$, $p < .001$, $\chi^2/df = 3.57$, TLI = .809, CFI = .864, RMSEA = .103, AIC = 160.14. This was significantly poorer than the three-dimension Model 1, $\Delta\chi^2_2 = 14.83$, $p < .001$, ΔAIC = 10.83. As such, Model 1 was considered the superior model.



Model 1



Model 1a



Model 1b

Appendix K: Study 3a full list of measures

Perceived algorithmic surveillance accuracy:

In my view, algorithmic surveillance…

1. ... is accurate at identifying people
2. ... creates an accurate impression of internet users
3. ... does not identify people's characteristics accurately
4. ... does not provide an accurate impression of internet users

Group-based recognition:

Distinctiveness:

1. Algorithmic surveillance enables society to recognise that gay people are a unique group
2. Algorithmic surveillance does not recognise the unique characteristics of gay people
3. From algorithmic surveillance, society recognises that gay people have distinct needs
4. Targeted adverts and web page suggestions often conflate my sexuality with my gender identity

Perceived stereotyping:

1. From using algorithmic surveillance society recognises diversity within the gay community

2. Targeted adverts and web page suggestions imply all gay people are the same

Positivity:

1. Results of algorithmic surveillance offer a positive image of gay people
2. Targeted material from algorithmic surveillance does not portray gay people positively
3. Algorithmic surveillance helps promote the positive impact of gay culture within society
4. Gay people are valued positively through algorithmic surveillance

Understanding:

1. Algorithmic surveillance does not provide society with an accurate understanding of gay culture
2. Algorithmic surveillance helps society appreciate gay people's values
3. Algorithmic surveillance provides society with a good understanding of what gay people believe
4. Algorithmic surveillance does not provide a better understanding of gay people's views

Recognition as a group member:

1. Through algorithmic surveillance I believe I am identified as a gay individual
2. Algorithmic surveillance does not identify me as gay

Feelings towards surveillance:

Algorithmic surveillance makes me feel:

1. Worried
2. Calm
3. Anxious
4. Relaxed
5. Angry
6. Happy
7. Annoyed
8. Pleased
9. Uncomfortable
10. Comfortable
11. Hopeful
12. Dejected
13. Optimistic
14. Discouraged

Visibility (participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how algorithmic surveillance made them feel):

1. Invisible/Visible
2. Anonymous/Identifiable
3. Unobserved/Observed
4. Unknown/Known

Degree to which algorithmic surveillance is perceived to contribute to discrimination (Participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how they felt)

The use of algorithmic surveillance could made society's behaviour towards gay people…

1. Worse/Better
2. More hostile/More friendly
3. More intolerant/More tolerant
4. Colder/Warmer
5. More unfair/More fair

Surveiller trust:

1. I trust the organisations gathering my data online
2. Surveillance conducted online is for the benefit of the gay community
3. I do not believe those gathering my data online have good intentions
4. Surveillance online will not benefit the gay community

Privacy concern:

1. Surveillance online is an invasion of privacy
2. People have a right to use the internet without being surveilled
3. People's online data should not be private information
4. People shouldn't expect privacy when using the internet

Behaviour change intentions:

Algorithmic surveillance would…

1. …make me concerned about what I do online
2. …make me censor what I do online
3. …not change how I use the internet
4. …not affect what I do online

Demographics:

Hours per week spent online (open ended)

Age (open ended)

Gender

5. Man
6. Woman
7. Non-binary
8. Prefer not to say

Nationality (open ended)

Ethnicity

7. White
8. Mixed/Multiple ethnic groups
9. Asian/Asian British
10. Black/African/Caribbean/Black British
11. Arab
12. Other (open ended)

Membership to closed or private groups/forums online

3. Yes
4. No

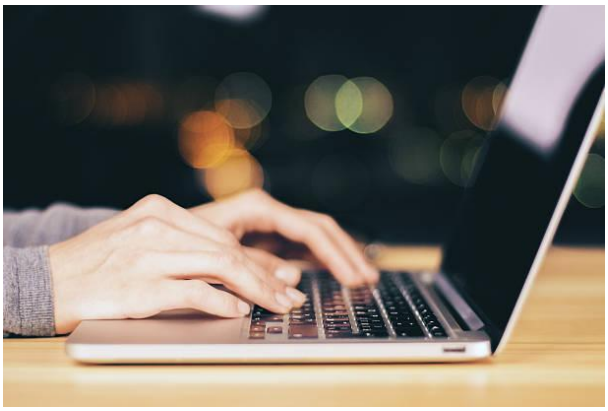
Awareness of algorithmic surveillance (1-10: 1 = *not at all aware,* 10 = *very aware*).

Openly gay:

1. Yes
2. No
3. To some people, but not others

Duration being openly gay (in years and months, open ended)

Appendix L: Stimulus text for Study 3a



Algorithmic surveillance is the storage and analysis of our online activity. For example, online shopping platforms will track what we buy, and media streaming services will track what we watch. This type of surveillance is also conducted by government agencies. Organisations like America's National Security Agency (NSA) and Britain's Government Communications Headquarters (GCHQ) have access to the majority of our digital activity. These agencies can track where we go (through geolocation software on our devices), who we call, what we post on social media, and much more. In addition to this, the corporate and state organisations do not operate independently. The government and the corporate world will often share data on groups of people between themselves.

These surveillance techniques allow both corporate and state organisations to make assumptions about who we are. Specifically, they estimate which demographic background we come from, including (but not limited to) our race, gender, and sexual orientation. This social sorting comes with other assumptions. For example, based on our demographic information, the government assesses who are likely threats to public order and safety. Alternatively, corporate organisations use our assumed background to calculate which products and services would be most appealing to us.

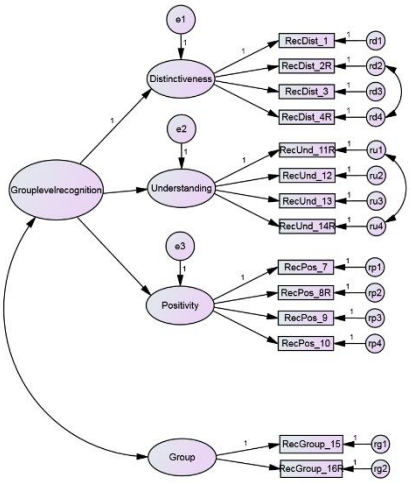
These assumptions can have a variety of social consequences. On a superficial level, how we are defined can determine what adverts we see online. For example, if you are assumed to be a woman, you may receive more ads for makeup and feminine clothing compared to an internet user assumed to be a man. But the consequences of surveillance can be far more profound than this. Algorithmic surveillance can determine what interest rates we are offered when we apply for a loan online. It can impact the cost of plane tickets and how quickly we can flag an Uber, or if we even get one at all. Algorithmic surveillance can also determine whether we are allowed past border control on our annual holiday. The collection of our data and how it is subsequently used can impact our lives well beyond our computer screens.

Appendix M: Confirmatory factor analysis for the group-based recognition measure

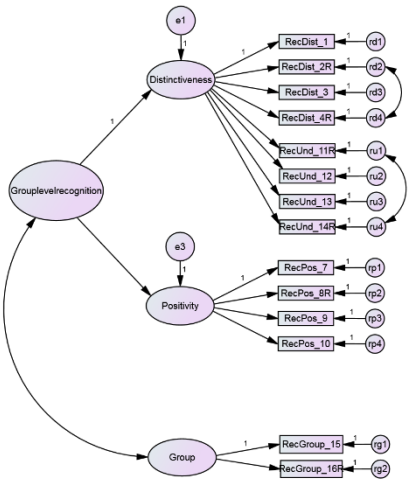
Confirmatory factor analysis was conducted to compare the hypothesised two second-order factors and three first-order factors structure (Model 1) with two more parsimonious structures, one containing only two first-order dimensions (Model 1a) and the other containing only two dimensions (Model 1b). Reverse coded items were covaried within each dimension to account for shared method variance.

Model 1 was tested as a baseline that could be compared with the more parsimonious models. Model 1 demonstrated acceptable fit, $\chi^2_{71} = 269.82$, $p < .001$, $\chi^2/df = 3.80$, TLI = .829, CFI = .903, RMSEA = .087, AIC = 337.82. Model 1a was then tested, which demonstrated also showed acceptable fit, $\chi^2_{72} = 305.90$, $p < .001$, $\chi^2/df = 4.25$, TLI = .855, CFI = .885, RMSEA = .094, AIC = 371.90, however this was significantly worse fit when compared with Model 1, $\Delta\chi^2_1 = 36.08$, $p < .001$, ΔAIC = 34.08.

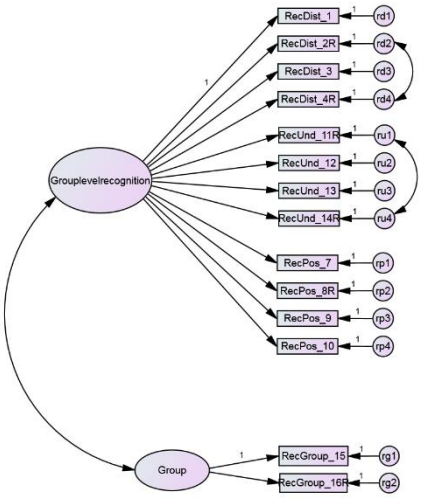
Model 1b was then tested and demonstrated adequate fit, $\chi^2_{74} = 362.31$, $p < .001$, $\chi^2/df = 4.90$, TLI = .826, CFI = .859, RMSEA = .103, AIC = 424.31. This was significantly poorer than Model 1, $\Delta\chi^2_3 = 92.49$, $p < .001$, ΔAIC = 86.49. As such, the hypothesised two second-order factor and three first-order factor model was considered superior.



Model 1



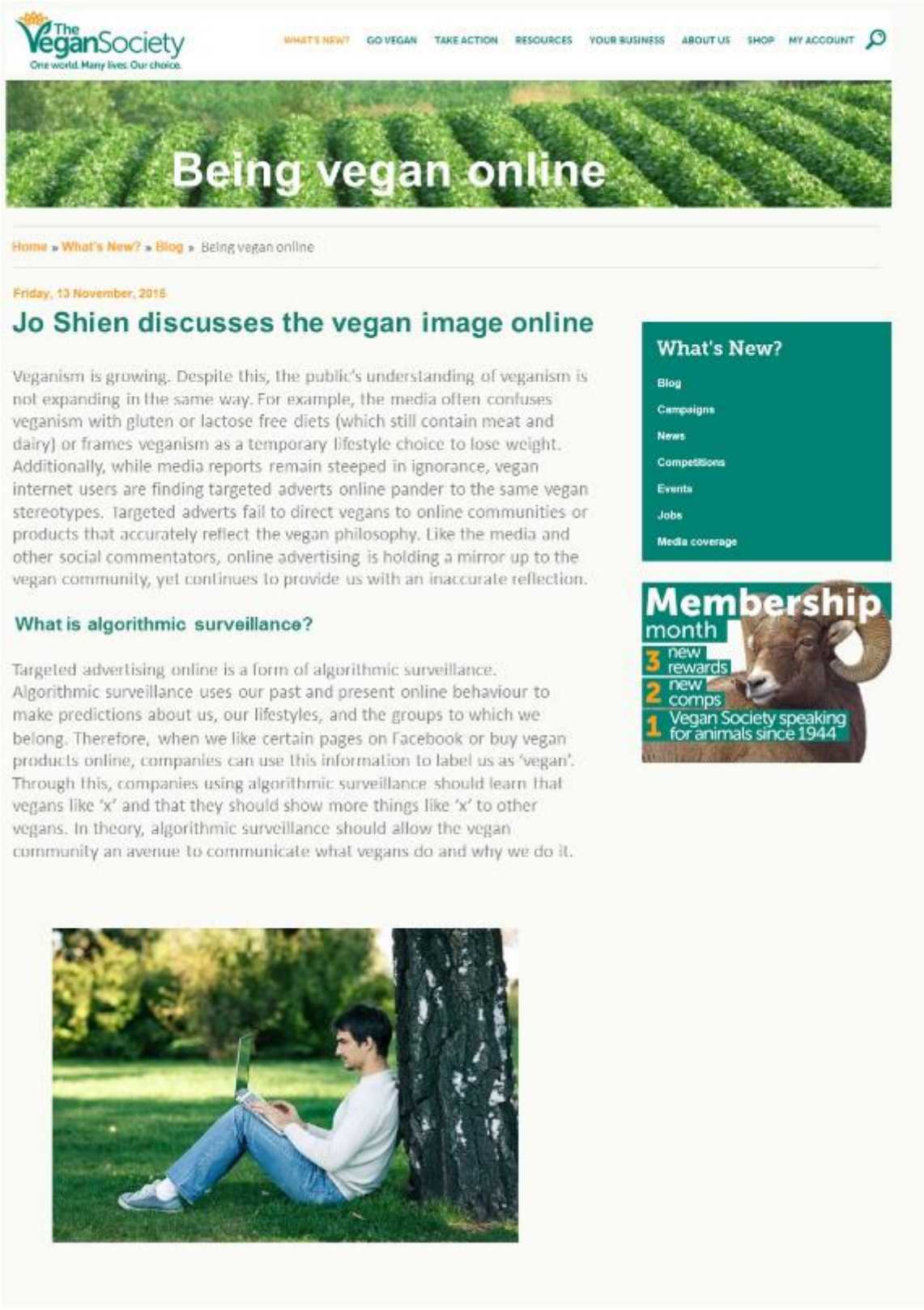
Model 1a



Model 1b

Appendix N: Study 3b manipulation materials

Page 1. Condition: low surveillance accuracy



Page 2. Condition: low surveillance accuracy

Page 1. Condition: medium surveillance accuracy

The Vegan Society
One world. Many lives. Our choice.

WHAT'S NEW? GO VEGAN TAKE ACTION RESOURCES YOUR BUSINESS ABOUT US SHOP MY ACCOUNT

Home » What's New? » Blog » Being vegan online

Friday, 13 November, 2015

Jo Shien discusses the vegan image online

Veganism is growing. Despite this, the public's understanding of veganism is not expanding in the same way. For example, the media often confuses veganism with gluten or lactose free diets (which still contain meat and dairy) or frames veganism as a temporary lifestyle choice to lose weight. While media reports remain steeped in ignorance, vegan internet users are finding targeted adverts online may or may not follow the same vegan stereotypes. Targeted adverts occasionally, but do not always, direct vegans to online communities or products that accurately reflect the vegan philosophy. Like the media and other social commentators, online advertising is holding a mirror up to the vegan community but only sometimes provides us with an accurate reflection.

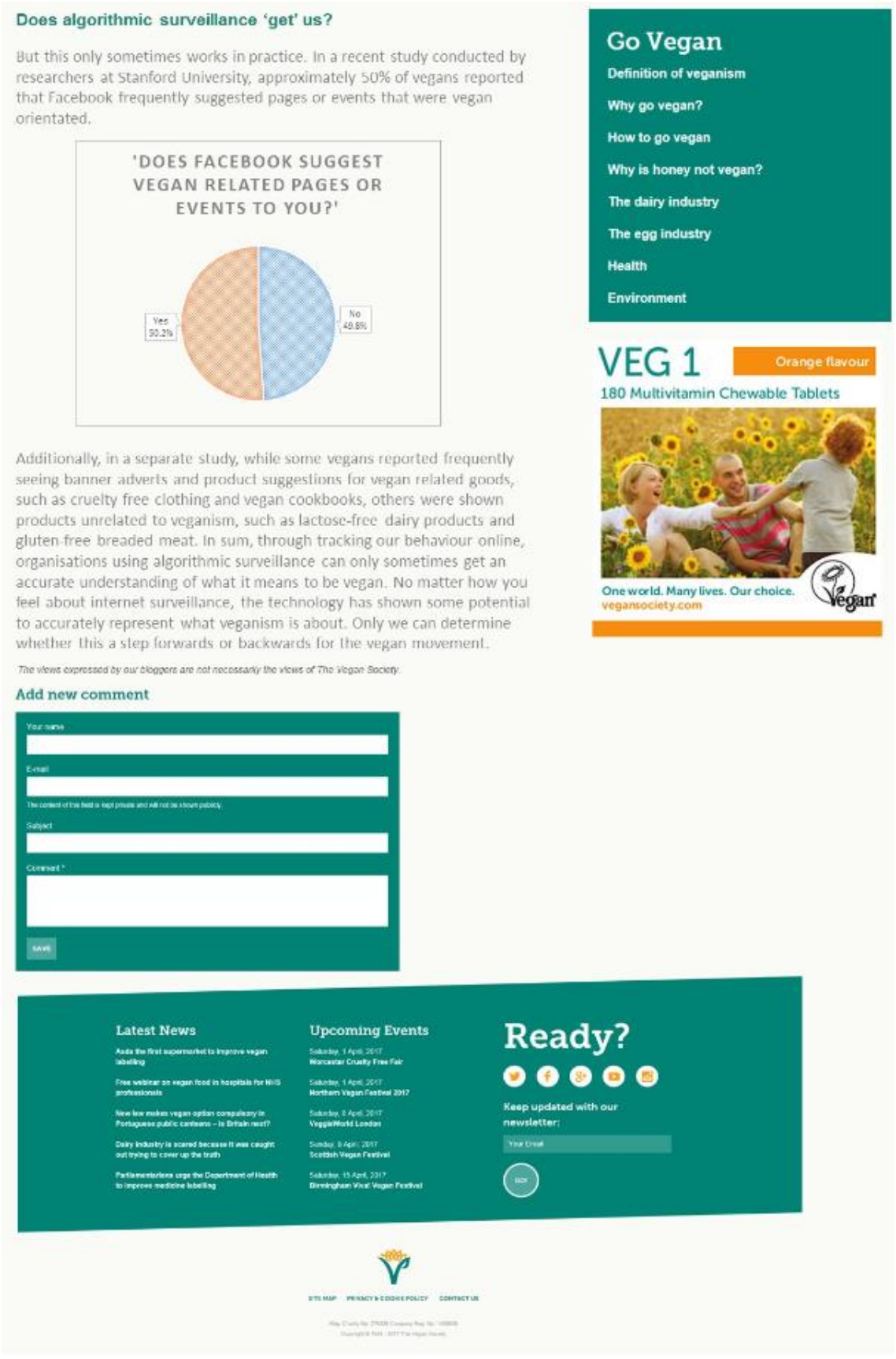
What is algorithmic surveillance?

Targeted advertising online is a form of algorithmic surveillance. Algorithmic surveillance uses our past and present online behaviour to make predictions about us, our lifestyles, and the groups to which we belong. Therefore, when we like certain pages on Facebook or buy vegan products online, companies can use this information to label us as 'vegan'. Through this, companies using algorithmic surveillance should learn that vegans like 'x' and that they should show more things like 'x' to other vegans. In theory, algorithmic surveillance should allow the vegan community an avenue to communicate what vegans do and why we do it.

What's New?

- Blog
- Campaigns
- News
- Competitions
- Events
- Jobs
- Media coverage

Page 2. Condition: medium surveillance accuracy



Page 1. Condition: high surveillance accuracy

The Vegan Society
One world. Many lives. Our choice.

WHAT'S NEW? GO VEGAN TAKE ACTION RESOURCES YOUR BUSINESS ABOUT US SHOP MY ACCOUNT

Being vegan online

Home » What's New? » Blog » Being vegan online

Friday, 13 November, 2015

Jo Shien discusses the vegan image online

Veganism is growing. Despite this, the public's understanding of veganism is not expanding in the same way. For example, the media often confuses veganism with gluten or lactose free diets (which still contain meat and dairy) or frames veganism as a temporary lifestyle choice to lose weight. However, while media reports remain steeped in ignorance, vegan internet users are finding targeted adverts online do not follow the same vegan stereotypes. Instead, targeted adverts are instrumental in directing vegans to online communities or products that accurately reflect the vegan philosophy. Like the media and other social commentators, online advertising is holding a mirror up to the vegan community, but is finally providing us with an accurate reflection.

What is algorithmic surveillance?

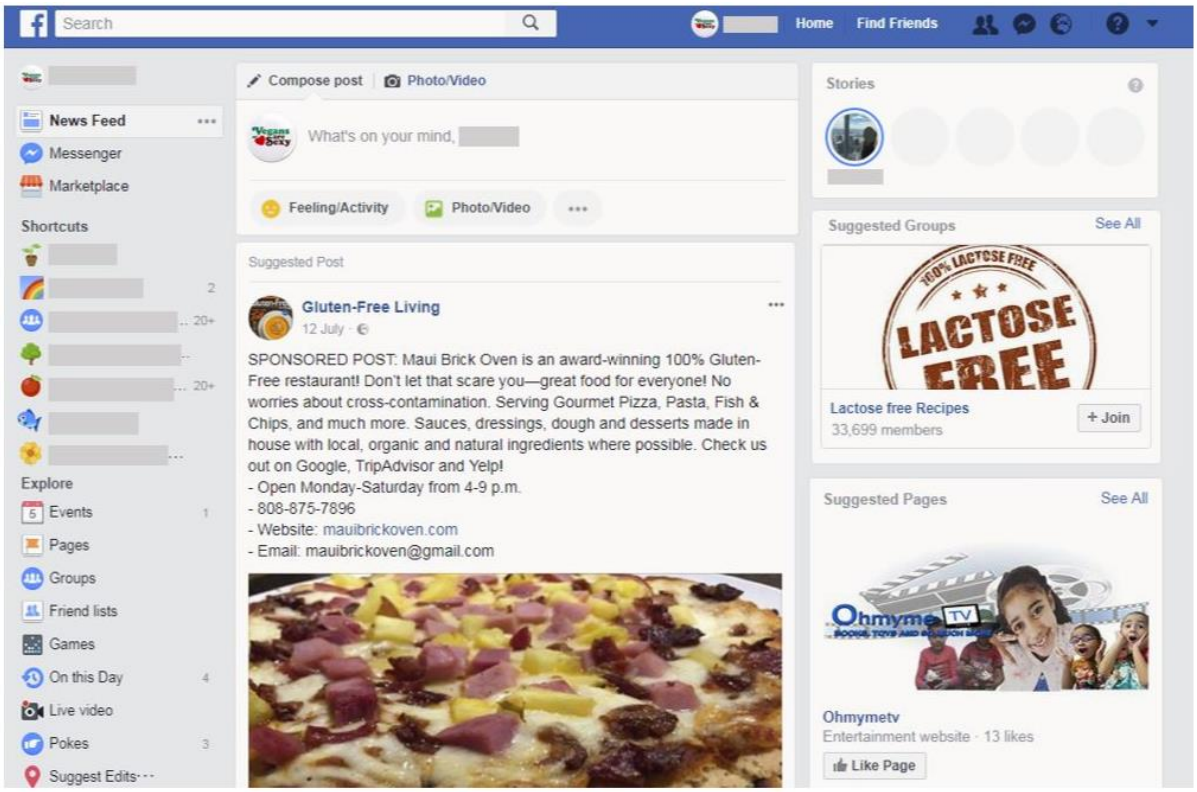
Targeted advertising online is a form of algorithmic surveillance. Algorithmic surveillance uses our past and present online behaviour to make predictions about us, our lifestyles, and the groups to which we belong. Therefore, when we like certain pages on Facebook or buy vegan products online, companies can use this information to label us as 'vegan'. Through this, companies using algorithmic surveillance should learn that vegans like 'x' and that they should show more things like 'x' to other vegans. In theory, algorithmic surveillance should allow the vegan community an avenue to communicate what vegans do and why we do it.

What's New?

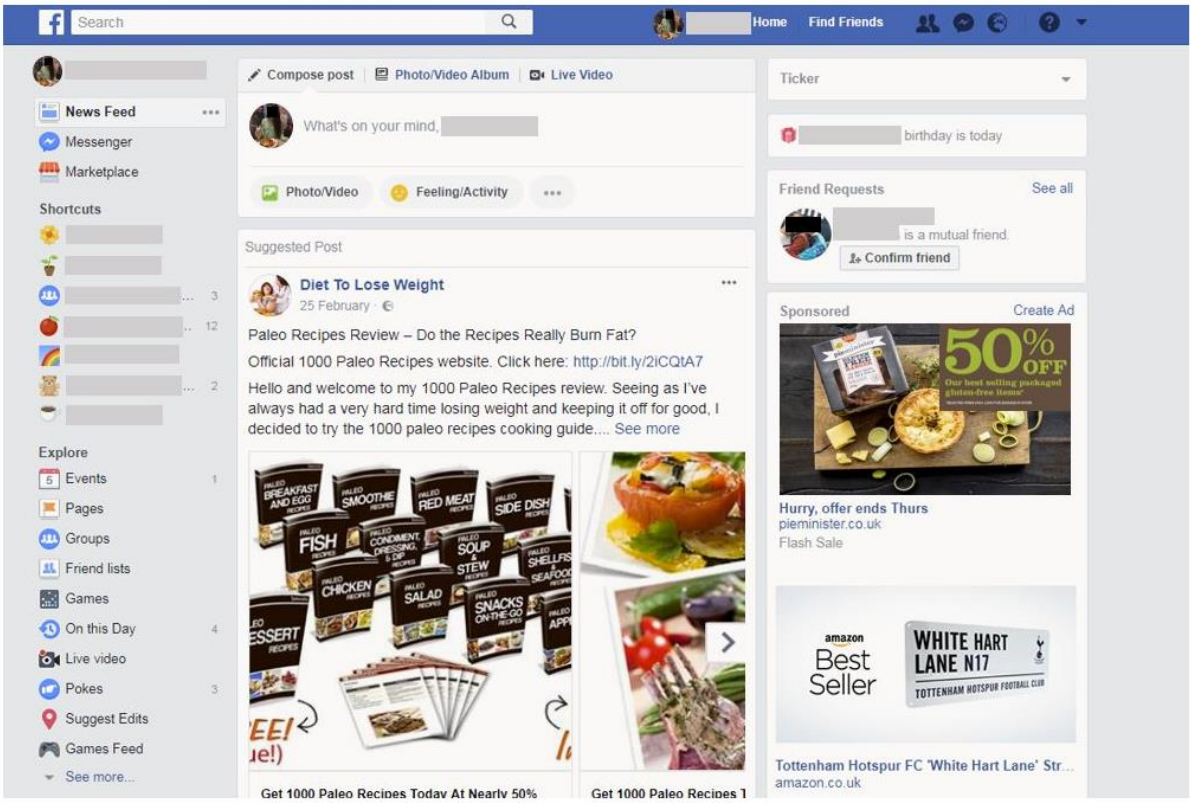
- Blog
- Campaigns
- News
- Competitions
- Events
- Jobs
- Media coverage

Page 2. Condition: high surveillance accuracy

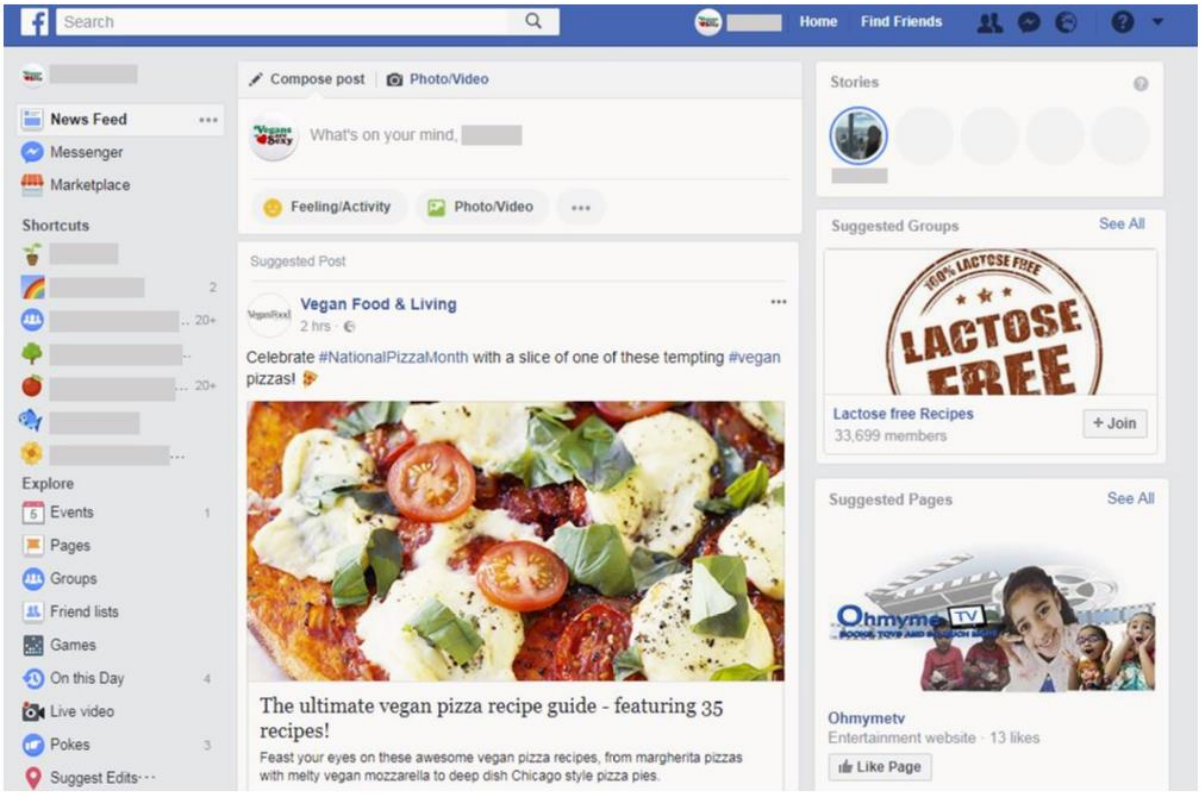
Low surveillance accuracy example 1



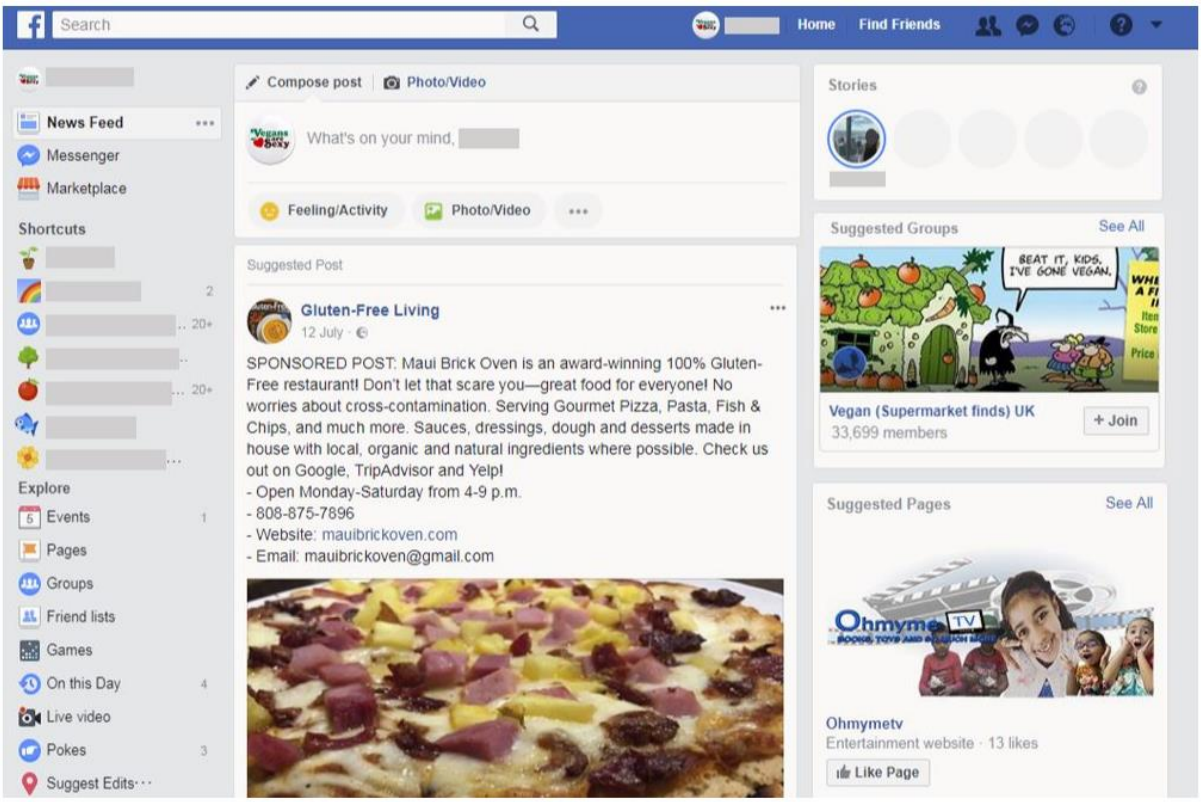
Low surveillance accuracy example 2



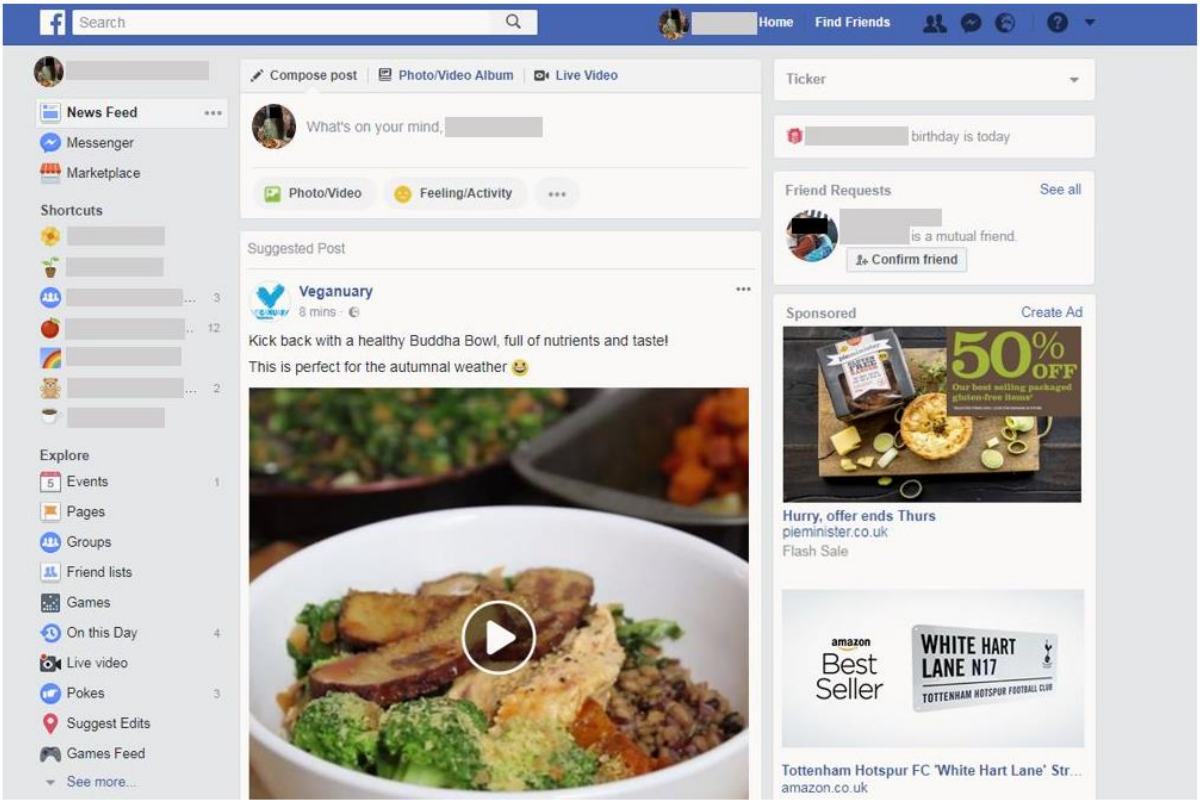
Medium surveillance accuracy example 1a



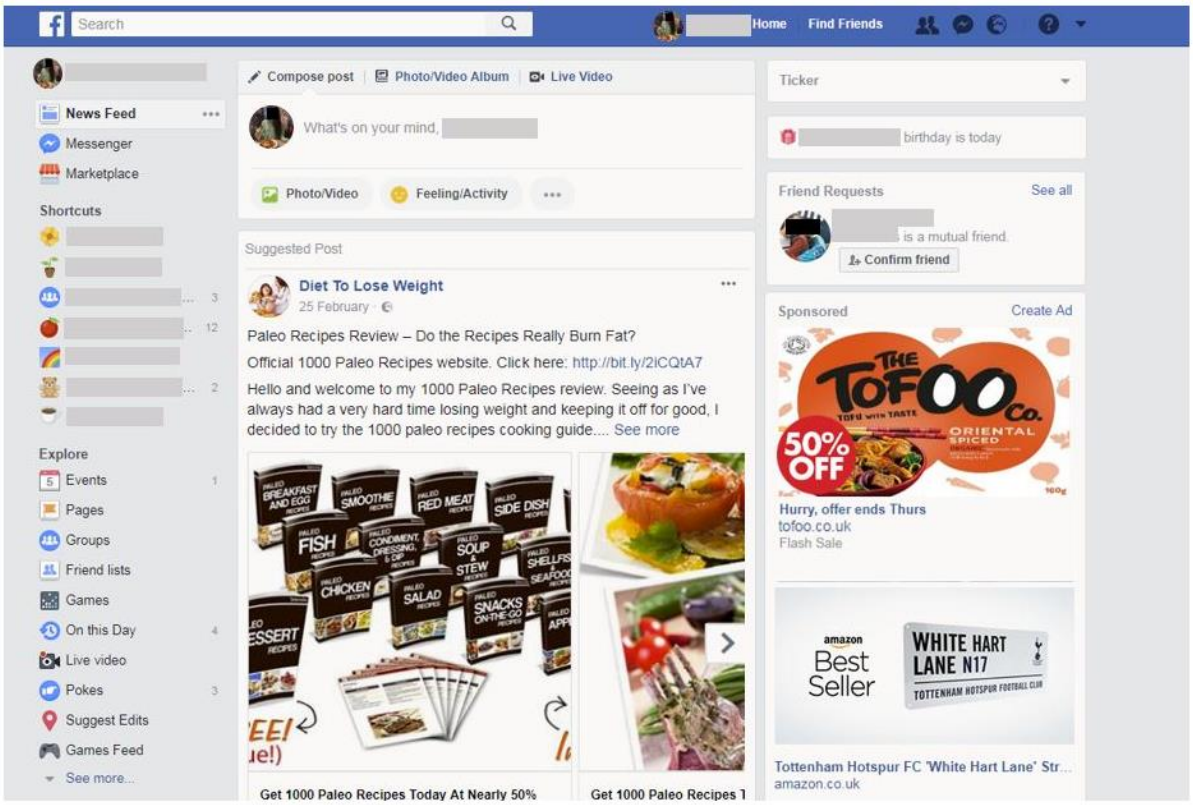
Medium surveillance accuracy example 1b



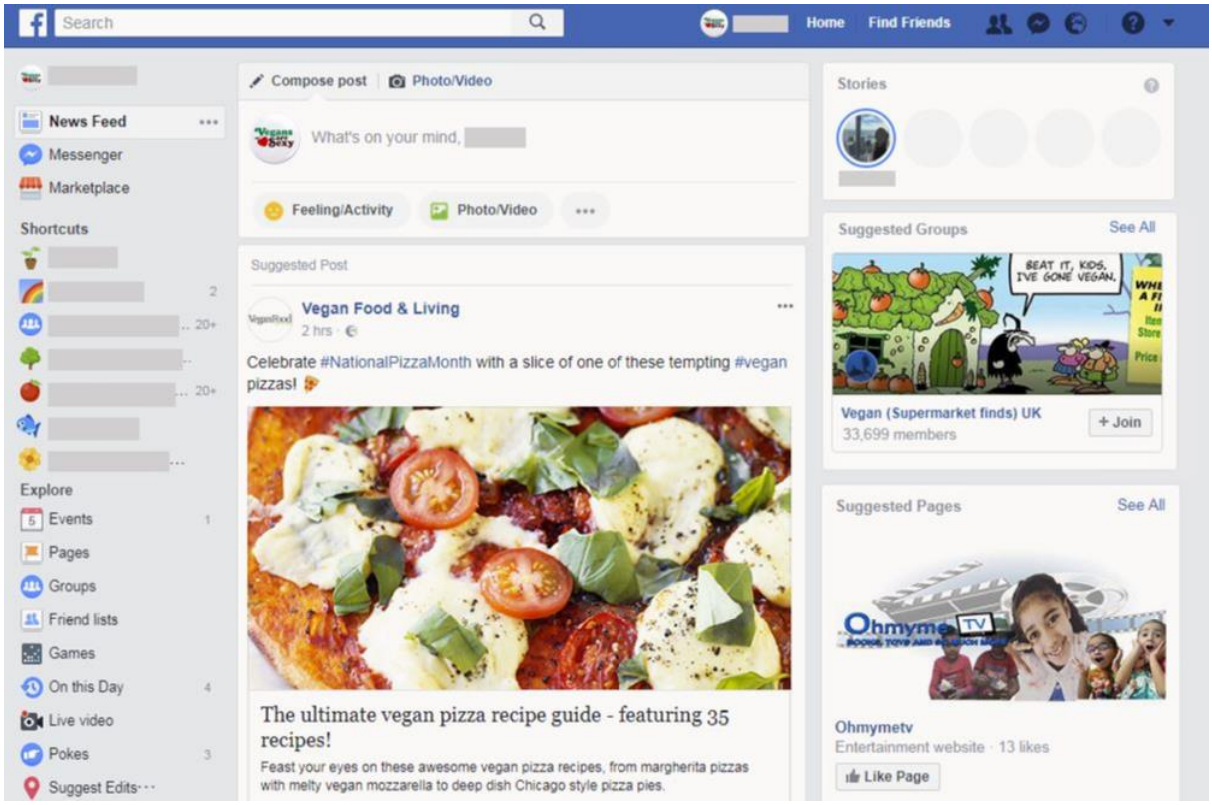
Medium surveillance accuracy example 2a



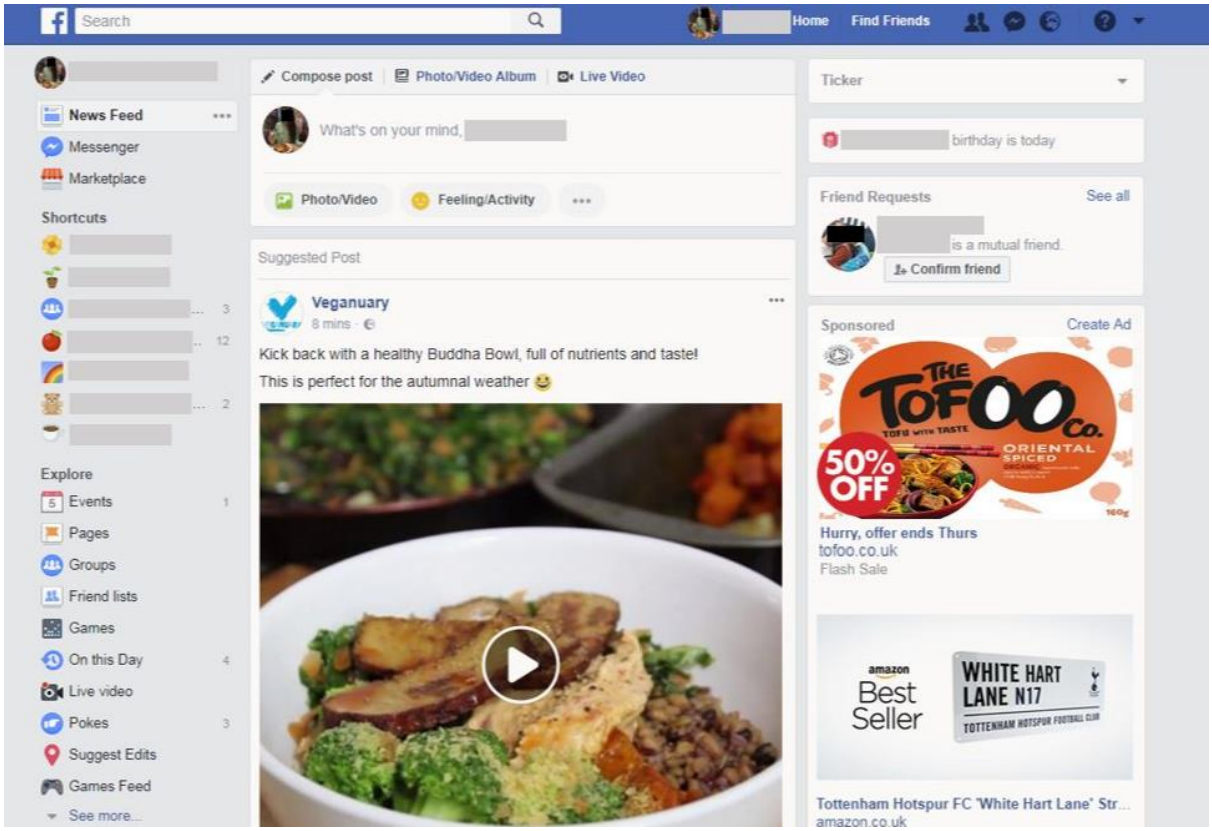
Medium surveillance accuracy example 2b



High surveillance accuracy example 1



High surveillance accuracy example 2



Appendix O: Study 3b full list of measures

Accuracy manipulation check (7-point Likert scale: 1 = *not accurate at all,* 7 = *Extremely accurate*):

1. The vegan Society article suggests that algorithmic surveillance is…
2. After reading the article, in my opinion algorithmic surveillance is…

Group-based recognition:

Distinctiveness:

1. Algorithmic surveillance enables omnivores to recognise that my beliefs towards food are distinct from those following other diets
2. Algorithmic surveillance may suggest that my diet is the same as diets unrelated to veganism (e.g. gluten-free diets)
3. By using algorithmic surveillance, omnivores may recognise that veganism is not about food intolerance/allergy
4. Targeted adverts and webpage suggestions imply that my diet is the same as 'clean eating'

Positivity:

1. The results of algorithmic surveillance offer a positive image of veganism
2. Targeted advertising does not portray veganism positively

Understanding:

1. Algorithmic surveillance does not provide omnivores with an accurate understanding of vegan culture
2. Algorithmic surveillance could help omnivores appreciate vegan cultural values
3. Algorithmic surveillance can provide omnivores with a good understanding of what vegans think
4. Algorithmic surveillance does not provide a better understanding of vegan views

Feelings towards surveillance:

Algorithmic surveillance makes me feel:

1. Worried
2. Calm
3. Anxious
4. Relaxed
5. Angry
6. Happy
7. Annoyed
8. Pleased
9. Uncomfortable
10. Comfortable
11. Hopeful
12. Dejected
13. Optimistic

14. Discouraged

Visibility (participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how algorithmic surveillance made them feel):

1. Invisible/Visible
2. Anonymous/Identifiable

Degree to which algorithmic surveillance is perceived to contribute to discrimination. (Participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how they felt)

Surveiller trust:

1. I trust the organisations gathering my data online
2. Surveillance conducted online is for the benefit of vegans
3. I do not believe those gathering my data online have good intentions
4. Surveillance online will not benefit vegans

Privacy concern:

1. Surveillance online is an invasion of privacy
2. People have a right to use the internet without being surveilled
3. People's online data is not private information
4. People shouldn't expect privacy when using the internet

Behaviour change intentions:

Algorithmic surveillance would…

1. …make me concerned about what I do online
2. …make me censor what I do online
3. …not change how I use the internet
4. …not affect what I do online

Demographics:

Hours per week spent online (open ended)

Age (open ended)

Gender

1. Male
2. Female
3. Non-binary
4. Prefer not to say

Nationality (open ended)

Ethnicity

1. White
2. Mixed/Multiple ethnic groups
3. Asian/Asian British
4. Black/African/Caribbean/Black British
5. Arab
6. Other (open ended)

Membership to closed or private groups/forums online

1. Yes
2. No

Awareness of algorithmic surveillance (1-10: 1 = *not at all aware,* 10 = *very aware*).

Duration vegan (year and months, open ended)

Trustworthiness of the article (7-point Likert scale: 1 = *strongly disagree,* 7 = *strongly agree)*

1. The online article was trustworthy
2. The information in the online article was not believable

The most important reason for going vegan (participants were asked to select just one answer):

1. Health
2. Animal welfare
3. Environmental reasons
4. Economic reasons
5. Taste preferences
6. Intolerance/allergy
7. Weight related reasons
8. Personal finances
9. Cultural/religious reasons
10. Other (open ended)

Appendix P: Confirmatory factor analyses of the group-based recognition measure

Confirmatory factor analysis was conducted to compare our hypothesised factor structure (Model 1) with a more parsimonious two sub-dimension model (Model 1a). The two-sub-dimension model was then tested against a single factor structure (Model 1b). We then used the preferred model to assess whether accuracy is a distinct dimension as predicted, or a component within the recognition structure. To do this, accuracy was included as an additional factor (Model 2). This model was then compared to a model in which the accuracy items were contained in either the distinctiveness dimension (Model 2a) and the positivity dimension (Model 2b). Model diagrams are illustrated in Figure 1.

First, Model 1 was tested to form a baseline. This was then used as a comparison model against the more parsimonious structures: Model 1a and Model 1b. Model 1 demonstrated poor fit, $\chi^2_{32} = 364.03$, $p < .001$, $\chi^2/df = 11.38$, TLI = .651, CFI = .752, RMSEA = .159, AIC = 410.03. However, analysis of the modification indices suggested shared method variance between the positively worded understanding pair (items 2 and 3; MI = 42.20, EPC = .33), the negatively worded understanding pair (items 1 and 4; MI = 46.91, EPC = .36), and the negatively worded distinctiveness pair (items 2 and 4; MI = 63.42, EPC = .68). This covariance likely represents an artefact of measurement (wording of survey items) rather than the underlying latent structure. As such, the error terms for each pair were covaried. The modified model was then tested, $\chi^2_{29} = 158.84$, $p < .001$, $\chi^2/df = 5.48$, TLI = .849, CFI = .903, RMSEA = .105, AIC =

210.84, which proved to be a significantly better fit than the original Model 1, $\Delta\chi^2_3 = 205.19$, $p < .001$, $\Delta AIC = 199.19$.

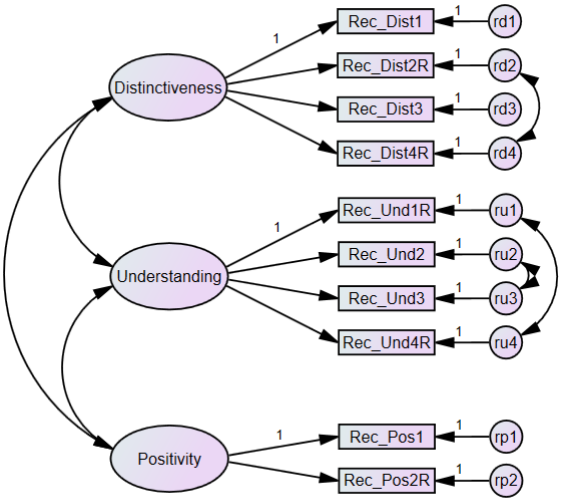
Model 1a was then assessed, which also showed acceptable fit, $\chi^2_{31} = 163.04$, $p < .001$, $\chi^2/df = 5.26$, TLI = .857, CFI = .901, RMSEA = .102, AIC = 211.04. However, the two-factor model did not have a significantly worse fit than the predicted three factor model, $\Delta \chi^2_2 = 4.2$, $p = .123$, $\Delta AIC = 0.2$. As model 1a provides a more parsimonious solution, the two-factor model, comprised of the distinctiveness and positivity dimensions, is considered preferable.

A single-factor structure was then tested, whereby all items loaded on to a single recognition factor (Model 1b). The model demonstrated poor fit, $\chi^2_{32} = 246.81$, $p < .001$, $\chi^2/df = 7.71$, TLI = .774, CFI = .839, RMSEA = .128, AIC = 292.81, and demonstrated significantly worse fit than the two-dimension structure $\Delta \chi^2_1 = 83.77$, $p < .001$, $\Delta AIC = 81.77$. As such, of the three model, Model 1a proved to be the most parsimonious model with the best fit. This model was then used to assess the independence of the accuracy measure from the recognition measure.

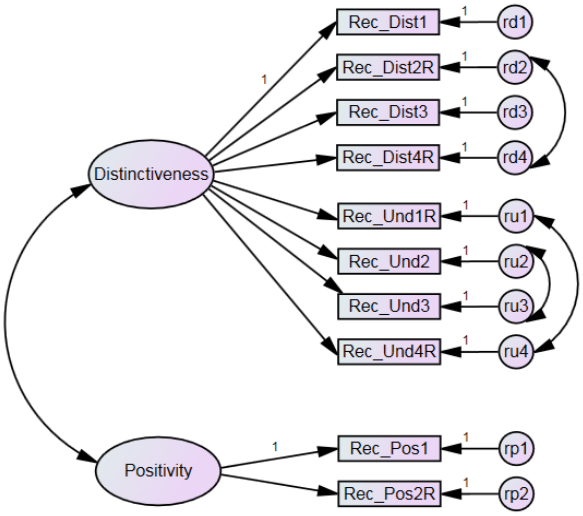
Model 2 served as a baseline for this comparison, in which accuracy was included as a third dimension. The model demonstrated acceptable fit, $\chi^2_{48} = 219.11$, $p < .001$, $\chi^2/df = 4.57$, TLI = .868, CFI = .904, RMSEA = .093, AIC = 279.11. This was then compared to Model 2a, where the accuracy items were included within the distinctiveness dimension. Model 2a showed poor fit, $\chi^2_{50} = 349.64$, $p < .001$, $\chi^2/df = 6.99$, TLI = .777, CFI = .831, RMSEA = .121, AIC = 405.64, and proved significantly worse than Model 2, $\Delta \chi^2_2 = 130.53$, $p < .001$, $\Delta AIC = 126.53$.

Lastly, Model 2 was compared to Model 2b, whereby the accuracy items were included in the positivity dimension. Model 2b showed poor fit, $\chi^2_{50} =$

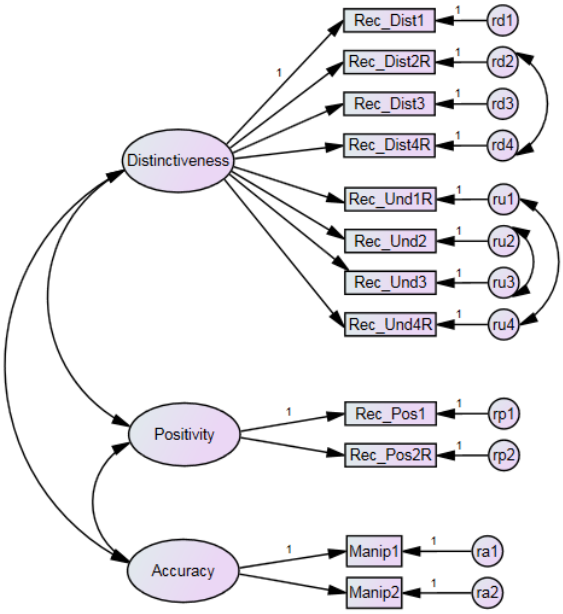
306.49, $p < .001$, $\chi^2/df = 6.13$, TLI = .810, CFI = .856, RMSEA = .112, AIC = 362.49. This was significantly poorer than the three-factor solution, $\Delta \chi^2_2 = 87.38$, $p < .001$, ΔAIC = 83.38. Together, this suggests that the accuracy perception items measure a distinct accuracy construct, which is independent from the recognition construct.



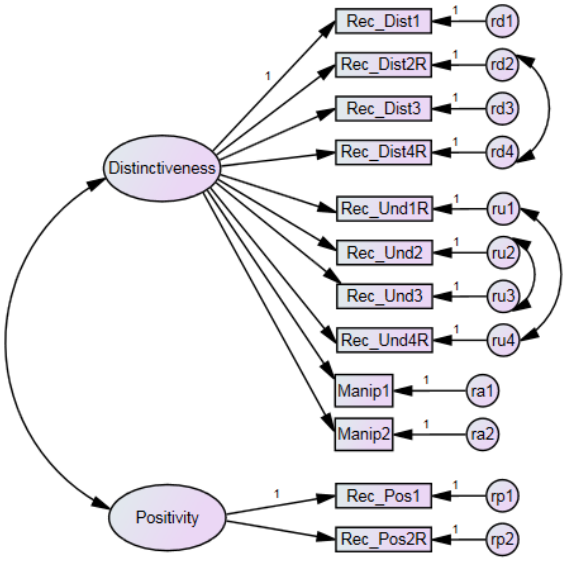
Model 1



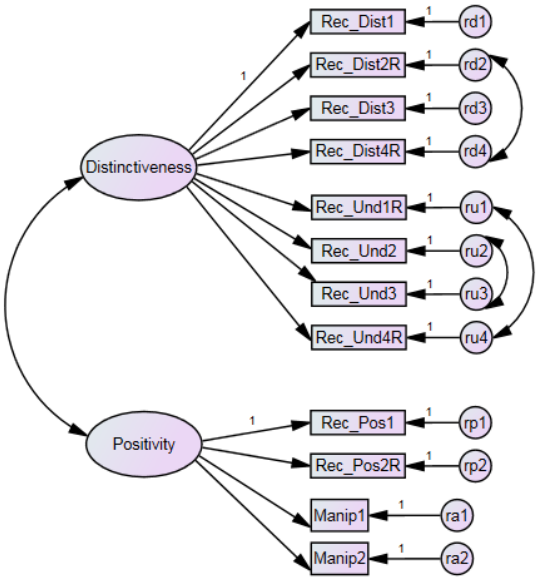
Model 1a



Model 2



Model 2a



Model 2b

Appendix Q: Study 4 manipulation materials

Misrecognition:

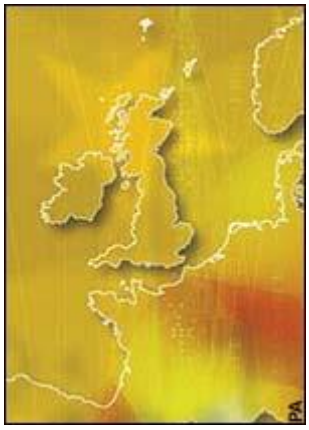
Wales – an invisible nation?

Within the UK and beyond, Welsh national identity is poorly understood, or even treated as invisible altogether. As one of the four countries that constitute the UK, Wales has a unique identity and culture, which sets it apart from the Scottish, Northern Irish/Irish, and English. Welsh teams compete in national and global sports leagues, and Welsh people have made a unique contribution in making the world a better place. For example, Aneurin Bevan was a Welshman who championed free healthcare for all, and his legacy and spirit created the foundations of the NHS today. Welsh artistic culture – both in the Welsh language and in English – is also vibrant. All of this and more can be celebrated on St David's day, an event that symbolises the unique heritage and resilience of the Welsh as a people. But to the wider world, it can seem as if Wales is barely on the map at all (quite literally).

Despite being a distinct nationality, the Welsh are rarely recognised as such. For example, many Welsh people have had the experience of being mistaken as English when travelling. To further rub salt in the wound, highlighting one's Welsh nationality is often met with the question 'so is that in England?'. It's no surprise that the wider world doesn't recognise the distinctiveness of Wales and Welshness, when previous depictions of the UK have erased Wales entirely from the map (see below). But this is nothing new. Welsh contributions down the years have been written out of history, including Wales' vital contributions to the British Empire at home and abroad. The Welsh background of many great individuals is also written out of their story: the

philosopher Bertrand Russell, the author Roald Dahl, the Paralympian and politician Tanni Grey-Thompson, and the comedian Tommy Cooper are some of the many great figures born in Wales, but who are more readily recognised as British or even English.

The failure to recognise Wales and Welshness as something positive and distinct from England and Englishness is also not unique to the past: as you read this, Welsh heritage is quite literally being re-written. Guidebooks for some of the most beautiful places in Wales are renaming locations to make pronunciation easier for people outside of Wales. Llyn Bochlwyd, a stunning lake in the mountains of Eryri has been conveniently re-named ‘Lake Australia’ – simply because it’s shaped like Australia. Taken together, this illustrates that the Welsh suffer chronic misrecognition, often being seen as either English, of vaguely British descent, or simply non-existent.



Recognition:

Wales – a celebrated nation

Within the UK and beyond, Welsh national identity is increasingly understood and respected. As one of the four countries that constitute the UK,

Wales has a unique identity and culture, which sets it apart from the Scottish, Northern Irish/Irish, and English. Welsh teams compete in national and global sports leagues, and Welsh people have made a unique contribution in making the world a better place. For example, Aneurin Bevan was a Welshman who championed free healthcare for all, and his legacy and spirit created the foundations of the NHS today. Welsh artistic culture – both in the Welsh language and in English – is also vibrant. All of this and more can be celebrated on St David's day, an event that symbolises the unique heritage and resilience of the Welsh as a people. And it seems the wider world are joining in on the celebrations too.

Wales is frequently recognised as a distinct nationality. For example, St David's day is celebrated in Argentina, Hong Kong, USA, France, and Australia. Wales and its uniqueness are well and truly on the map. Our global presence is also bolstered by Welsh people's contributions throughout history that are widely recognised: the philosopher Bertrand Russell, the author Roald Dahl, the Paralympian and politician Tanni Grey-Thompson, and the comedian Tommy Cooper are hailed as some of the greatest Welsh people to have lived. The importance of their Welsh background is also increasingly recognised – for example, the statue of Tommy Cooper in Caerphilly, and Roald Dahl Plass (plaza) in the heart of Cardiff Bay. Moreover, Tanni Grey-Thompson was awarded the Dame title (DBE) in recognition of her contribution to sport and was described by Clare Balding from the BBC as 'one of the best Welsh Olympians we have seen to date – she does Wales and Great Britain proud'.

The recognition of Wales and Welshness is also present elsewhere. In 2017, Lonely Planet named Wales in the top 5 of places to visit in the world on their annual Best in Travel list. Areas in Wales ranked above regions of

Australia and Malaysia. Additional recognition has been found in pop-culture. Marvel's blockbuster triumph, Black Panther, celebrated Welsh distinctiveness by displaying the Welsh flag (Y Ddraig Goch) in a scene set at a United Nations conference amongst the flags of other global powerhouses. Since 2005, Google have also celebrated St David's Day with their iconic Google 'Doodle' – the logo that appears when opening their search engine. Designs often include treasured symbols, such as the daffodil and the dragon (below). In sum, the Welsh are embraced in many facets of life, and our unique spirit is seen as setting us apart from our British neighbours.

Low surveillance accuracy:

We are all familiar with targeted advertising online. It is a form of algorithmic surveillance that uses our past and present online behaviour to

make predictions about us, our lifestyles, and the groups to which we belong. However, in a recent survey, 89% of Welsh people stated that most suggested material online miscategorised them as English. This means that for most Welsh people, algorithms fail to identify their nationality as distinct, or they do not identify the Welsh individual as being a member of their nationality. Either way, adverts targeted at Welsh people have predominantly English content, which frequently promote events related to English events (e.g. St George's day) and will often be geared towards English sport and culture more generally. The inaccuracy of surveillance is shown below with four screenshots taken from Welsh people's Facebook pages.

In sum, online algorithms rarely view the Welsh identity as a nationality in its own right. So no matter how you feel about internet surveillance, the technology has shown little potential to accurately represent what Welsh people are about.

Medium surveillance accuracy:

We are all familiar with targeted advertising online. It is a form of algorithmic surveillance that uses our past and present online behaviour to make predictions about us, our lifestyles, and the groups to which we belong. In a recent survey, 50% of Welsh people stated that most suggested material online accurately identified them as Welsh. On the other hand, the other 50% of Welsh people surveyed stated that most suggested material online miscategorised them as English. This means that for half of Welsh people online, algorithms fail to identify their nationality as distinct, or they do not identify the Welsh individual as being a member of their nationality. Whereas for the other half of Welsh users online, the Welsh identity is seen as distinct and they are also perceived as a Welsh person. Consequently, whilst some of us may see predominantly English content which promotes English culture, the rest of us will see content tailored to our Welsh identity. The hit and miss nature of surveillance is shown below with four screenshots taken from Welsh people's Facebook pages.

In sum, online algorithms only occasionally view the Welsh identity as a nationality in its own right. So no matter how you feel about internet

surveillance, the technology has shown only some potential to accurately represent what Welsh people are about.

High surveillance accuracy:

We are all familiar with targeted advertising online. It is a form of algorithmic surveillance that uses our past and present online behaviour to make predictions about us, our lifestyles, and the groups to which we belong. In a recent survey, 89% of Welsh people stated that most suggested material online accurately identified them as Welsh. This means that for the majority of Welsh people, algorithms successfully identify their nationality as distinct, and also perceived them as a Welsh individual. This demonstrates that adverts

targeted at Welsh people have predominantly Welsh content, which frequently promote events related to Welsh events (e.g. St David's day) and will often be geared towards Welsh sport and culture more generally. The accuracy of surveillance is shown below with four screenshots taken from Welsh people's Facebook pages.

In sum, online algorithms typically view the Welsh identity as a nationality in its own right. So no matter how you feel about internet surveillance, the technology has shown the potential to accurately represent what Welsh people are about.

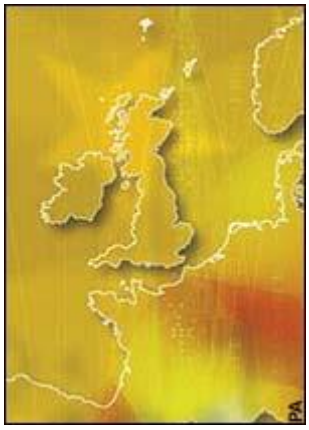
Cymru – cenedl anweladwy?

Yn y DU a thu hwnt, ceir diffyg dealltwriaeth o hunaniaeth genedlaethol Cymru, neu caiff ei thrin yn gwbl anweladwy. Fel un o bedair gwlad y DU, mae gan Gymru ei hunaniaeth a'i diwylliant unigryw, sy'n ei gosod ar wahân i'r Alban, Gogledd Iwerddon/Iwerddon a Lloegr. Mae timau o Gymru yn cystadlu mewn cynghreiriau chwaraeon cenedlaethol a byd-eang, ac mae'r Cymry wedi cyfrannu'n unigryw at wneud y byd yn lle gwell. Er enghraifft, roedd Aneurin Bevan yn Gymro a hyrwyddodd gofal iechyd am ddim i bawb, a'i waddol a'i ysbryd ef osododd sylfeini'r GIG heddiw. Mae diwylliant artistig Cymru – trwy gyfrwng y Gymraeg a'r Saesneg – hefyd yn hyfyw. Gellir dathlu hyn oll a mwy ar ddydd Gŵyl Dewi, digwyddiad sy'n symbol o dreftadaeth unigryw a chadernid y Cymry fel pobl. Ond i'r byd ehangach, prin yr ymddengys bod Cymru ar y map o gwbl (yn eithaf llythrennol).

Er gwaethaf y ffaith eu bod yn genedl ar wahân, anaml iawn y caiff y Cymry eu cydnabod felly. Er enghraifft, mae llawer o Gymry wedi cael y profiad o gael eu camgymryd yn Saeson wrth deithio. I roi halen ar y briw, mae tynnu sylw at eich cenedlaetholdeb Cymreig yn aml yn arwain at y cwestiwn 'felly a yw yn Lloegr?'. Nid yw'n syndod nad yw'r byd ehangach yn adnabod arwahanrwydd Cymru a Chymreictod, pan fo portreadau blaenorol o'r DU wedi dileu Cymru o'r map yn llwyr (gweler isod). Ond nid rhywbeth newydd yw hyn. Cafodd cyfraniadau Cymru drwy'r oesoedd eu dileu o hanes, gan gynnwys cyfraniadau hollbwysig Cymru at yr Ymerodraeth Brydeinig gartref a thramor. Mae llinach Gymreig llawer o enwogion hefyd wedi'i dileu o'u hanes: yr athronydd Bertrand Russell, yr awdur Roald Dahl, y pencampwr Paralympaidd

a’r gwleidydd Tanni Grey-Thompson, a’r digrifwr Tommy Cooper yw rhai o’r bobl enwog niferus a anwyd yng Nghymru ond a gaiff eu hadnabod fel Prydeinwyr neu Saeson hyd yn oed.

Nid yw’r methiant i gydnabod bod Cymru a Chymreictod yn rhywbeth cadarnhaol ac ar wahân i Loegr a Seisnigrwydd yn unigryw i’r gorffennol ychwaith: wrth ichi ddarllen hwn, mae treftadaeth Cymru yn llythrennol yn cael ei hailysgrifennu. Mae llyfrau twristiaeth i rai o leoedd hyfrytaf Cymru yn ailenwi lleoliadau i’w gwneud yn haws i bobl y tu allan i Gymru eu hynganu. Cafodd Llyn Bochlwyd, llyn hynod ym mynyddoedd Eryri, ei ailenwi’n gyfleus yn ‘Lake Australia’ – oherwydd bod ei siâp yn debyg i siâp Awstralia. At ei gilydd, mae hyn yn dangos bod y Cymry yn dioddef camadnabyddiaeth cronig, ac yn aml yn cael eu hystyried yn Saeson, yn lled Brydeinig, neu nid ydynt yn bodoli o gwbl.



Recognition in Welsh:

Cymru – cenedl a ddethlir

Yn y DU a thu hwnt, ceir dealltwriaeth gynyddol o hunaniaeth genedlaethol Cymru, a pharch cynyddol tuag ati. Fel un o bedair gwlad y DU, mae gan Gymru ei hunaniaeth a’i diwylliant unigryw, sy’n ei gosod ar wahân i’r

Alban, Gogledd Iwerddon/Iwerddon a Lloegr. Mae timau o Gymru yn cystadlu mewn cynghreiriau chwaraeon cenedlaethol a byd-eang, ac mae'r Cymry wedi cyfrannu'n unigryw at wneud y byd yn lle gwell. Er enghraifft, roedd Aneurin Bevan yn Gymro a hyrwyddodd gofal iechyd am ddim i bawb, a'i waddol a'i ysbryd ef osododd sylfeini'r GIG heddiw. Mae diwylliant artistig Cymru – trwy gyfrwng y Gymraeg a'r Saesneg – hefyd yn hyfyw. Gellir dathlu hyn oll a mwy ar ddydd Gŵyl Dewi, digwyddiad sy'n symbol o dreftadaeth unigryw a chadernid y Cymry fel pobl. Ac mae'r byd ehangach i'w weld yn ymuno yn y dathlu hwn hefyd.

Caiff Cymru ei hadnabod yn aml fel gwlad â chenedligrwydd arbennig. Er enghraifft, caiff dydd Gŵyl Dewi ei ddathlu yn yr Ariannin, Hong Kong, UDA, Ffrainc, ac Awstralia. Mae unigrywiaeth Cymru yn sicr ar y map. Rhoddir hwb i'n presenoldeb byd-eang hefyd gan gyfraniadau pobl Cymru drwy gydol hanes ac fe'i cydnabyddir yn eang: caiff yr athronydd Bertrand Russell, yr awdur Roald Dahl, y pencampwr Paralympaidd a gwleidydd Tanni Grey-Thompson, a'r digrifwr Tommy Cooper eu henwi yn rhai o bobl enwocaf Cymru erioed. Ceir cydnabyddiaeth gynyddol hefyd o bwysigrwydd eu llinach Gymreig – er enghraifft, y cerflun o Tommy Cooper yng Nghaerffili, a Phlas Roald Dahl yng nghanol Bae Caerdydd. Yn ogystal â hyn, dyfarnwyd teitl Bonesig (DBE) i Tanni Grey-Thompson i gydnabod ei chyfraniad at fyd chwaraeon ac fe'i disgrifiwyd gan Clare Balding o'r BBC yn un o bencampwyr Olympaidd gorau Cymru hyd yn hyn – mae hi'n destun balchder i Gymru a Phrydain Fawr.

Gwelir cydnabyddiaeth o Gymru a Chymreictod mewn mannau eraill hefyd. Yn 2017, cafodd Cymru ei henwi yn un o'r pum lle gorau yn y byd i ymweld â nhw ar y rhestr flynyddoedd o leoedd gorau i deithio yn y cylchgrawn Lonely Planet. Daeth ardaloedd o Gymru yn uwch ar y rhestr na rhannau o

Awstralia a Malaysia. Hefyd, ceir cydnabyddiaeth ym myd diwylliant poblogaidd. Dathlodd y ffilm fawr gan Marvel, Black Panther, arwahanrwydd Cymru trwy ddangos baner Y Ddraig Goch mewn golygfa a leolwyd yng nghynhadledd y Cenhedloedd Unedig ymysg baneri gwledydd mawr eraill y byd. Ers 2005, mae Google hefyd wedi dathlu Dydd Gŵyl Dewi gyda'i Google 'Doodle' eiconig – y logo sydd i'w weld wrth agor ei beiriant chwilio. Mae dyluniadau yn aml yn cynnwys symbolau annwyl, fel y genhinen Pedr a'r ddraig (isod). I grynhoi, caiff y Cymry eu dathlu mewn llawer o agweddau ar fywyd, ac ystyrir bod ein hysbryd unigryw yn ein gosod ar wahân i'n cymdogion ym Mhrydain.

Low surveillance accuracy in Welsh:

Mae pob un ohonom yn gyfarwydd â hysbysebion targedu ar-lein. Mae'n fath o wyliadwriaeth algorithmig sy'n defnyddio ein hymddygiad ar-lein yn y gorffennol a'r presennol i lunio rhagfynegiadau amdanom ni, ein ffordd o fyw, a'r grwpiau yr ydym yn perthyn iddyn nhw. Fodd bynnag, mewn arolwg diweddar, dywedodd 89% o'r Cymry fod y rhan fwyaf o ddeunydd ar-lein a awgrymir iddyn nhw yn eu cam-gategoreiddio fel Saeson. Felly, i'r rhan fwyaf o Gymry, mae

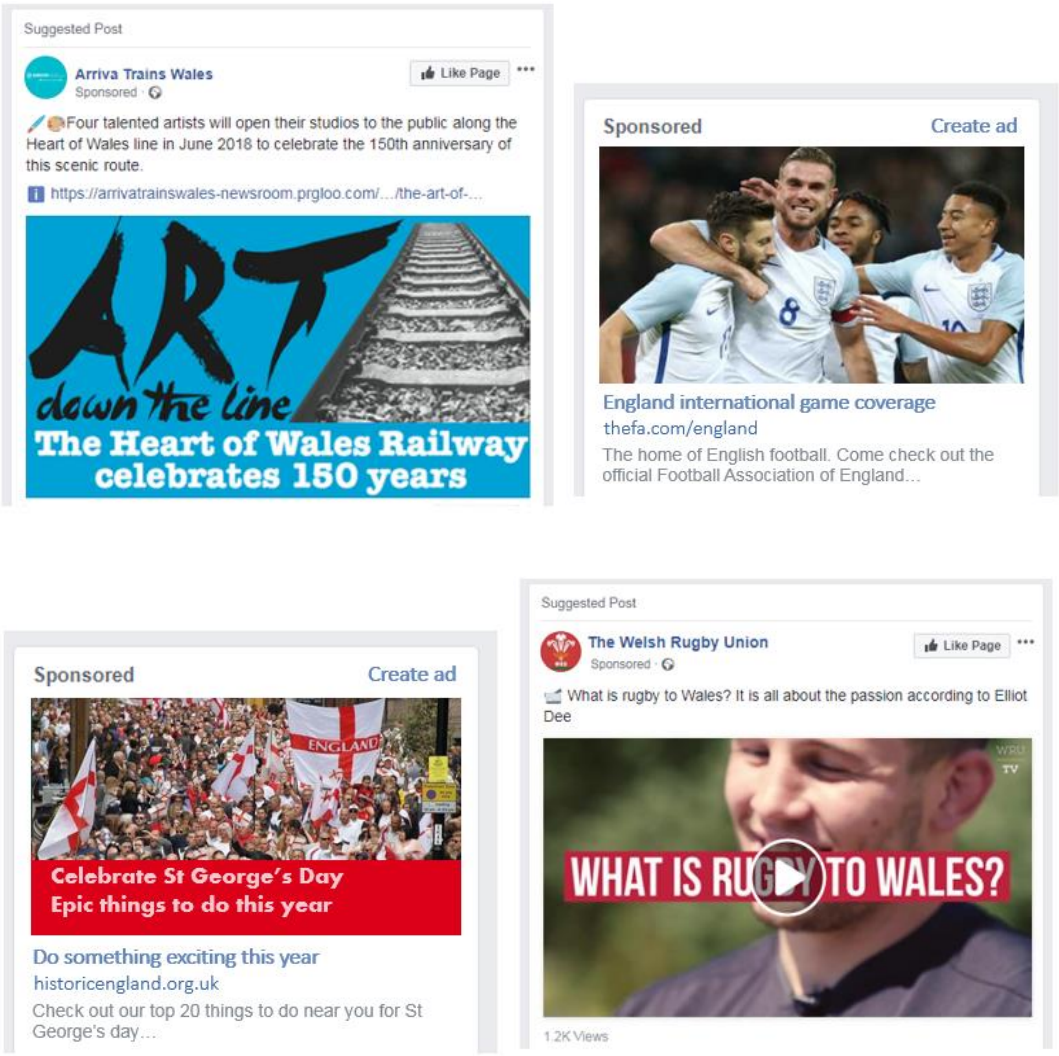
algorithmau yn methu ag adnabod bod eu cenedligrwydd yn unigryw, neu'n methu ag adnabod bod yr unigolyn o Gymru yn aelod o'i genedl. Y naill ffordd neu'r llall, mae hysbysebion sy'n targedu'r Cymry yn cynnwys deunydd sy'n ymwneud i raddau helaeth â Lloegr, sy'n aml yn hyrwyddo digwyddiadau sy'n berthnasol i Loegr (e.e. Dydd San Siôr) a byddant yn aml yn canolbwyntio ar chwaraeon a diwylliant Lloegr yn fwy cyffredinol. Dangosir isod anghywirdeb gwyliadwriaeth mewn pedwar ciplun o dudalennau Facebook pobl o Gymru.

I grynhoi, yn anaml y bydd algorithmau ar-lein yn ystyried hunaniaeth Cymru yn genedligrwydd yn ei rhinwedd ei hun. Felly, ni waeth beth yw eich teimladau ynghylch gwyliadwriaeth ar y rhyngrwyd, potensial prin a ddangoswyd gan y dechnoleg i gynrychioli'r Cymry yn gywir.

Medium surveillance accuracy in Welsh:

Mae pob un ohonom yn gyfarwydd â hysbysebion targed ar-lein. Mae'n fath o wyliadwriaeth algorithmig sy'n defnyddio ein hymddygiad ar-lein yn y gorffennol a'r presennol i lunio rhagfynegiadau amdanom ni, ein ffordd o fyw, a'r grwpiau yr ydym yn perthyn iddyn nhw. Mewn arolwg diweddar, dywedodd 50% o'r Cymry fod y rhan fwyaf o ddeunydd ar-lein a awgrymir iddynt yn eu hadnabod fel Cymry. Ar y llaw arall, dywedodd y 50% arall o'r Cymry a arolygwyd fod y rhan fwyaf o ddeunydd ar-lein a awgrymir iddynt yn eu cam-gategoreiddio fel Saeson. Felly, i hanner y Cymry ar-lein, mae algorithmau yn methu ag adnabod eu cenedligrwydd fel rhywbeth ar wahân, neu'n methu ag adnabod yr unigolyn o Gymru fel aelod o'i genedl. Ond i'r hanner arall o Gymry ar-lein, ystyrir bod hunaniaeth Cymru yn rhywbeth arbennig a'u bod yn Gymry. O ganlyniad, er y bydd rhai ohonom yn gweld deunydd Saesnig yn bennaf sy'n hyrwyddo diwylliant Lloegr, bydd y gweddill ohonom yn gweld deunydd sydd wedi'i deilwra i'n hunaniaeth Gymreig. Dangosir isod natur ddidaro gwyliadwriaeth mewn pedwar ciplun o dudalennau Facebook pobl o Gymru.

I grynhoi, dim ond ar brydiau y bydd algorithmau ar-lein yn ystyried hunaniaeth Cymru yn genedligrwydd yn ei rhinwedd ei hun. Felly, ni waeth beth yw eich teimladau ynghylch gwyliadwriaeth ar y rhyngrwyd, rhywfaint yn unig o botensial a ddangoswyd gan y dechnoleg i gynrychioli'r Cymry yn gywir.

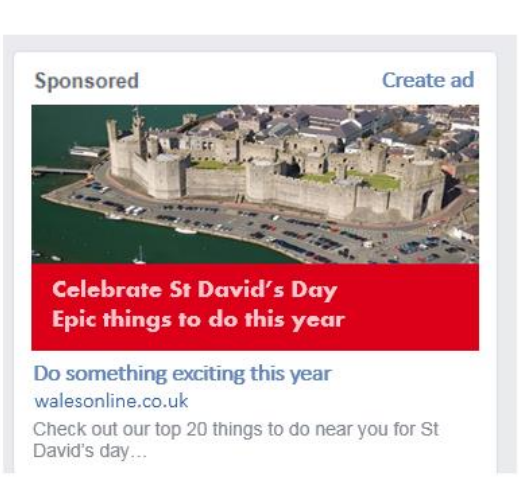


High surveillance accuracy in Welsh:

Mae pob un ohonom yn gyfarwydd â hysbysebion targed ar-lein. Mae'n fath o wyliadwriaeth algorithmig sy'n defnyddio ein hymddygiad ar-lein yn y gorffennol a'r presennol i lunio rhagfynegiadau amdanom ni, ein ffordd o fyw, a'r grwpiau yr ydym yn perthyn iddyn nhw. Mewn arolwg diweddar, dywedodd 89% o'r Cymry fod y rhan fwyaf o ddeunydd ar-lein a awgrymir iddyn nhw yn eu hadnabod yn gywir fel Cymry. Felly, i'r mwyafrif o'r Cymry, mae algorithmau yn adnabod bod eu cenedligrwydd fel rhywbeth ar wahân, ac yn eu hadnabod fel Cymro/Cymraes. Mae hyn yn dangos bod hysbysebion sydd wedi'u targedu at y

Cymry yn cynnwys deunydd sy'n berthnasol i Gymru ar y cyfan, sy'n aml yn hyrwyddo digwyddiadau sy'n berthnasol i ddigwyddiadau yng Nghymru (e.e. Dydd Gŵyl Dewi) a bydd yn aml yn ymwneud â chwaraeon a diwylliant Cymru yn fwy cyffredinol. Dangosir isod gywirdeb gwyliadwriaeth mewn pedwar ciplun o dudalennau Facebook pobl o Gymru.

I grynhoi, yn nodweddiadol bydd algorithmau ar-lein yn ystyried hunaniaeth Cymru yn genedligrwydd yn ei rhinwedd ei hun. Felly, ni waeth beth yw eich teimladau ynghylch gwyliadwriaeth ar y rhyngrwyd, mae'r dechnoleg wedi dangos y potensial i gynrychioli'r Cymry yn gywir.



Appendix R: Study 4 full list of measures

Group-based recognition manipulation check:

1. The article suggested that Welsh people are well recognised by wider society
2. Those outside Wales recognise that the Welsh nationality is distinct
3. Wider society recognises diversity amongst Welsh people
4. Welsh people are valued positively by wider society
5. Society understands Welsh people's views
6. Welsh people are mistreated by wider society
7. I am typically identified as a Welsh individual

Surveillance accuracy manipulation check:

In my view, algorithmic surveillance…

1. ...is accurate at identifying people
2. ...creates an accurate impression of internet users
3. ...does not identify people's characteristics accurately
4. ...does not provide an accurate impression of internet users
5. The article suggested that algorithmic surveillance accurately identifies Welsh people

Group-based recognition:

Distinctiveness:

1. Algorithmic surveillance enables society to recognise that Welsh people are a unique nationality
2. Algorithmic surveillance does not recognise the unique characteristics of Welsh people
3. From algorithmic surveillance, society may recognise that Welsh people have distinct needs
4. Targeted adverts and web page suggestions often imply I am English

Perceived stereotyping:

1. From using algorithmic surveillance, society can recognise diversity amongst Welsh people
2. Targeted adverts and web page suggestions imply all Welsh people are the same

Positivity:

1. The results of algorithmic surveillance offer a positive image of Welsh people
2. targeted material from algorithmic surveillance does not portray Welsh people positively
3. Algorithmic surveillance helps promote the positive impact of Welsh culture within wider society
4. Welsh people are valued positively through algorithmic surveillance

Understanding:

1. Algorithmic surveillance does not provide society with an accurate understanding of Welsh culture
2. Algorithmic surveillance helps wider society appreciate Welsh people's values
3. Algorithmic surveillance provides wider society with a good understanding of what Welsh people believe
4. Algorithmic surveillance does not provide a better understanding of Welsh people's views

Recognition as a group member:

1. Through algorithmic surveillance, I believe I am identified as a Welsh individual
2. Algorithmic surveillance does not identify me as Welsh.

Feelings towards surveillance:

Algorithmic surveillance makes me feel…

1. Worried
2. Calm
3. Anxious
4. Relaxed
5. Angry
6. Happy

7. Annoyed
8. Pleased
9. Uncomfortable
10. Comfortable
11. Hopeful
12. Dejected
13. Optimistic
14. Discouraged

Visibility (participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how algorithmic surveillance made them feel):

1. Invisible/Visible
2. Anonymous/Identifiable
3. Unobserved/Observed
4. Unknown/Known

Degree to which algorithmic surveillance is perceived to contribute to discrimination. (Participants were asked to select a point (7-point scale) between the adjectives to indicate which best described how they felt)

The use of algorithmic surveillance could make society's behaviour towards Welsh people…

1. Worse/Better
2. More hostile/More friendly

3. More intolerant/More tolerant
4. Colder/Warmer
5. More unfair/More fair

Surveiller trust:

1. I trust the organisations gathering my data online
2. Surveillance conducted online is for the benefit of Welsh people
3. I do not believe those gathering my data online have good intentions
4. Surveillance online will not benefit Welsh people

Privacy concern:

1. Surveillance online is an invasion of privacy
2. People have a right to use the internet without being surveilled
3. People's online data is not private information
4. People shouldn't expect privacy when using the internet

Behaviour change intentions:

Algorithmic surveillance would…

1. …make me concerned about what I do online
2. …make me censor what I do online
3. …not change how I use the internet
4. …not affect what I do online

Demographics:

Hours per week spent online (open ended)

Age (open ended)

Gender

1. Woman
2. Man
3. Non-binary
4. Prefer not to say

Ethnicity

1. White
2. Mixed/Multiple ethnic groups
3. Asian/Asian British
4. Black/African/Caribbean/Black British
5. Arab
6. Other (open ended)

Membership to closed or private groups/forums online

1. Yes
2. No

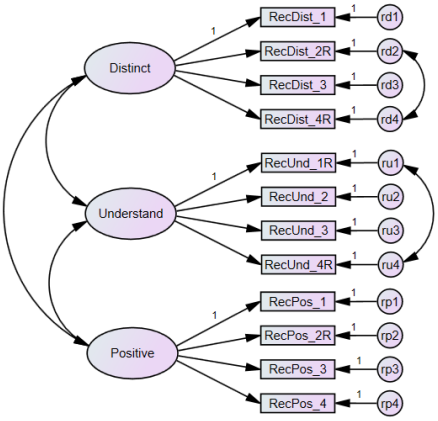
Awareness of algorithmic surveillance (1-10: 1 = *not at all aware,* 10 = *very aware*).

Appendix S: Confirmatory factor analysis for the group-based recognition measure

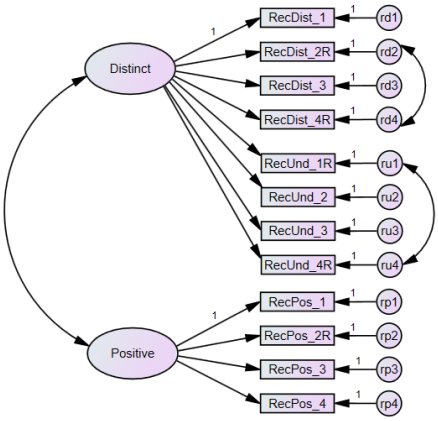
Confirmatory factor analysis was conducted to compare the hypothesised three-dimension structure (Model 1) with two variants of a more parsimonious two-dimension structure (Model 1a and Model 1b). Reverse coded items were covaried within each dimension to account for shared method variance.

Model 1 was tested as a baseline that could be compared with the two-dimension models. Model 1 demonstrated acceptable fit, $\chi^2_{49} = 278.74$, $p < .001$, $\chi^2/df = 5.69$, TLI = .904, CFI = .929, RMSEA = .109, AIC = 336.74. Model 1a was then tested, which demonstrated poor fit, $\chi^2_{51} = 356.96$, $p < .001$, $\chi^2/df = 7.00$, TLI = .877, CFI = .905, RMSEA = .124, AIC = 410.96, and had significantly worse fit when compared with Model 1, $\Delta\chi^2_2 = 78.22$, $p < .001$, ΔAIC = 74.22.

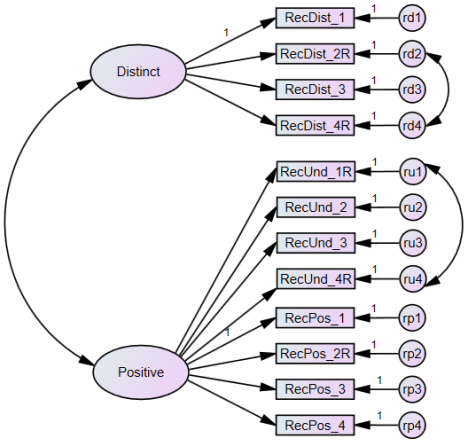
Model 1b was then tested and demonstrated poor fit, $\chi^2_{51} = 435.85$, $p < .001$, $\chi^2/df = 8.55$, TLI = .845, CFI = .880, RMSEA = .139, AIC = 489.85. This was significantly poorer than the three-dimension Model 1, $\Delta\chi^2_2 = 157.11$, $p < .001$, ΔAIC = 153.11. As such, Model 1 was considered the superior model.



Model 1



Model 1a



Model 1b